IRPP choices

Vol. 15, no. 5, June 2009 ISSN 0711-0677

Assessing the Secrecy Rules

Craig Forcese

IRPP

Founded in 1972, the Institute for Research on Public Policy is an independent, national, nonprofit organization.

IRPP seeks to improve public policy in Canada by generating research, providing insight and sparking debate that will contribute to the public policy decision-making process and strengthen the quality of the public policy decisions made by Canadian governments, citizens, institutions and organizations.

IRPP's independence is assured by an endowment fund established in the early 1970s.

Fondé en 1972, l'Institut de recherche en politiques publiques est un organisme canadien, indépendant et sans but lucratif.

L'IRPP cherche à améliorer les politiques publiques canadiennes en encourageant la recherche, en mettant de l'avant de nouvelles perspectives et en suscitant des débats qui contribueront au processus décisionnel en matière de politiques publiques et qui rehausseront la qualité des décisions que prennent les gouvernements, les citoyens, les institutions et les organismes canadiens.

L'indépendance de l'IRPP est assurée par un fonds de dotation établi au début des années 1970.

The opinions expressed in this paper are those of the author and do not necessarily reflect the views of IRPP or its Board of Directors.

Craig Forcese is an associate professor in the Faculty of Law at the University of Ottawa, where he teaches public international law, national security law, administrative law, and public law and legislation; he also runs the annual foreign policy practicum. Much of his present research and writing relates to international law, national security and democratic accountability. He is the author of *National Security Law: Canadian Practice in International Perspective* (2007). Prior to joining the University of Ottawa law faculty, he practised with Hughes Hubbard and Reed LLP, a Washington, DC, firm specializing in international trade law. He has law degrees from the University of Ottawa and Yale University, a BA from McGill University, and an MA in international affairs from the Norman Paterson School of International Affairs, Carleton University. He is a member of the Bars of Ontario, New York and the District of Columbia.

This publication was produced under the direction of Mel Cappe, President, IRPP, and Wesley Wark, Fellow, IRPP. The manuscript was copy-edited by Francesca Worrall, proofreading was by Mary Williams, production was by Chantal Létourneau, art direction was by Schumacher Design and printing was by AGL Graphiques.

Copyright belongs to IRPP. To order or request permission to reprint, contact:

IRPP
1470 Peel Street, Suite 200
Montreal, Quebec H3A 1T1
Telephone: 514-985-2461
Fax: 514-985-2559
E-mail: irpp@irpp.org
www.irpp.org

All *IRPP Choices* and *IRPP Policy Matters* are available for download at www.irpp.org

To cite this document:

Forcese, Craig. 2008. "Canada's National Security 'Complex': Assessing the Secrecy Rules." *IRPP Choices* 15 (5).

Security and Democracy / Sécurité et démocratie

Research Directors/Directeurs de recherche

Mel Cappe and/et Wesley Wark

This IRPP research program explores the complex challenges confronting Canada with regard to the post-9/11 security environment and its impact on domestic and international policies. The research addresses issues that are in many ways new to the country and to the formulation of Canadian national security policy, above all the threat posed by global, transnational terrorism. The program examines the interrelationships between new security demands and democratic norms, focusing in particular on the building blocks of a sound democratic model for national security, namely, effective intelligence; capable law enforcement; appropriate, stable laws; good governance; accountability; citizen engagement and public knowledge; emergency response capability; wise economic policy; and public-private-sector partnerships.

Ce programme de recherche s'intéresse aux défis de sécurité d'une grande complexité que le Canada doit relever depuis le 11 septembre, de même qu'à leur incidence sur nos politiques nationales et internationales. Il traitera d'enjeux souvent inédits pour notre pays en matière de sécurité nationale, notamment le terrorisme mondial et transnational. Le programme vise à analyser l'interrelation entre les nouvelles exigences de sécurité et les normes démocratiques, de manière à définir les éléments de base suivants : un modèle de sécurité nationale pleinement démocratique, notamment en matière de renseignement ; l'efficacité du maintien de l'ordre ; la stabilité et la légitimité des lois ; la gouvernance éclairée ; la responsabilisation ; l'engagement citoyen et l'information du public ; l'intervention d'urgence ; une politique économique avisée ; et les partenariats entre les secteurs public et privé.

Contents

2 List of Acronyms and Abbreviations
3 Introduction
4 Principles of Transparency
6 Principles of National Security Confidentiality
19 Reconciling Transparency and National Security Confidentiality
27 Conclusion and Recommendations
30 Notes
33 References
37 Résumé
38 Summary

List of Acronyms and Abbreviations

Access Act	*Access to Information Act*
ATA	*Anti-terrorism Act*
CEA	*Canada Evidence Act*
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
CSIS Act	*Canadian Security Intelligence Service Act*
SIRC	Security Intelligence Review Committee
CSE commissioner	Communications Security Establishment commissioner
DFAIT	Department of Foreign Affairs and International Trade
DND	Department of National Defence
FOIA	US *Freedom of Information Act*
IRPA	*Immigration Refugee Protection Act*
RCMP	Royal Canadian Mounted Police
SOIA	*Security of Information Act*

Canada's National Security "Complex":
Assessing the Secrecy Rules

Craig Forcese

Introduction

"Secrecy," said Cardinal Richelieu in 1641, "is the first essential in affairs of the State" (1641). Constraints on information disclosure may give governments a leg-up over their international rivals, preserve them from their enemies and insulate them from domestic opponents. Protection of the nation and its inhabitants may depend on keeping information about weapons systems, troop strengths, intelligence assets or physical vulnerabilities away from enemies. As the famous Second World War-era admonishment warned, "loose lips...sink ships."[1] For these reasons and others, "it is difficult to think of national security without also thinking about government secrecy" (Roberts 2004).

Of course, excessive secrecy may also be a vice in today's modern democracies. Information is, as the famous US Supreme Court Justice Louis Brandeis once quipped, "the best of disinfectants" (1914). Openness and transparency may preserve citizens from the malfeasance, incompetence, corruption and expedient behaviour of incumbent governments.

Relative latecomers to the open government concept, Canadians have a suspicion of government secrecy. Former auditor general of Canada Denis Desautels urged that "information is the current that charges accountability in government" (Information Commissioner of Canada 2001). Government accountability, in this view, requires timely and extensive access to government information. Without the capacity to compel disclosure of information unfavourable to government, citizens – including elected members of Parliament – are dependent on the potentially self-serving information the government chooses to release.

Indeed, secrecy, even when motivated by an objective as fundamental as national security, may sometimes create more perils than it forestalls. In 2003, the Standing Senate Committee on National Security and Defence released its report *The Myth of Security at Canada's Airports*. The study documented deeply inadequate security at Canadian airports, even in the post-

9/11 era, and concluded that "the front door of air security...[is] now being fairly well secured, with the side and back doors wide open" (2003, 9). In the course of preparing its report, the committee was "criticized for calling witnesses that have shared knowledge of these breaches with the Canadian public" (2003, 11). It rejected this criticism, observing:

> You can be sure that ships really will sink if they have a lot [*sic*] holes in them. And those holes aren't likely to get patched unless the public applies pressure to get the job done. They certainly aren't patched yet...The Committee recognizes the need to balance the public's right to know against the interests of national security. But unreasonable secrecy acts against national security. It shields incompetence and inaction, at a time that competence and action are both badly needed. (2003, 12-13)[2]

National security, in other words, is not about insulating governments from embarrassment.

In fact, the current director of the Canadian Security Intelligence Service (CSIS) has argued that excessive secrecy may also undermine the credibility of the government's national security policies. In his words, "there is a risk that, absent adequate public dialogue and a surfeit of secrecy, the justification for action by governments against terrorism will be undermined or misunderstood. This in turn can put in jeopardy the legitimacy of the government response" (Judd 2007). Security specialist Wesley Wark has echoed this concern: with injudicious secrecy, "credibility in the field of national security is undermined and the very idea of legitimate state secrets, often scoffed at by a Canadian public unused to the idea, is further eroded" (2007).

The dilemma of any government information regime lies in balancing the strong public interest in disclosure in all areas, including national security, against legitimate secrecy. As the 2003 Senate committee acknowledged, seeking assurances that secure doors at airports are actually locked is a proper public concern. Demanding disclosure of the combination codes to those doors would not be (Standing Senate Committee on National Security and Defence 2003, 12).

In this study I assess Canada's efforts to balance transparency with secrecy in the national security area. In the second section I highlight principles of transparency that animate the Canadian concepts of "open government" and "open courts." I then posit several principles of national security confidentiality – that is, justifications for secrecy predicated on national security preoccupations. I also describe how Canadian information laws seek to guard national security confidentiality. In the fourth section I assess how well Canadian information law reconciles national security with transparency, flagging a number of structural and practical problems that plague this reconciliation. I conclude with a number of recommendations as to how secrecy and transparency might be better reconciled in Canadian law and practice.

Principles of Transparency

The principles of transparency at the heart of Canadian information law and policy fall into two broad classes: "open government" and "open courts." In Canadian practice, open government involves the executive branch of government, while the open court concept relates to the judicial system (and to quasi-judicial bodies that, while technically part of the executive, have many of the trappings of courts).

Open government

Justification

The open government doctrine envisages access to information as an essential attribute of democracy. As one of the founders of the United States, James Madison, noted: "a popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy, or perhaps both. Knowledge will forever govern ignorance; And the people who mean to be their own Governors, must arm themselves with the power which knowledge gives" (letter to W.T. Barry, August 4, 1822, in Padover 1953).

Policy-makers voiced similar sentiments in discussions of what would become the United States *Freedom of Information Act (FOIA)*,[3] introduced as the world's first modern information access law in 1966. Proponents of the Act argued that "free people are, of necessity, informed; uninformed people can never be free."[4] In signing the *FOIA*, President Johnson noted that "this legislation springs from one of our most essential principles: A democracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest" ("Statement by the President" 1966). In a 1978 decision under the *FOIA*, the US Supreme Court echoed this comment, noting that "the basic purpose of *FOIA* is to ensure an informed citizenry, vital to

the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[5]

Unlike its immediate predecessor, the new Obama administration appears to share this perspective. One of the President's first acts was to issue a directive instructing federal agencies to act more transparently. That instrument reads, "transparency promotes accountability and provides information for citizens about what their Government is doing" (Presidential Documents 2009).

Canadians have expressed similar views during discussions of federal information access laws. Prime Minister Trudeau noted in 1975 that "democratic progress requires the ready availability of true and complete information. In this way people can objectively evaluate the government's policies. To act otherwise is to give way to despotic secrecy."[6] Then-president of the Privy Council Walter Baker underscored this point in 1979, urging that "if this Parliament is to function, if groups in society are to function, if the people of the country are to judge in a knowledgeable way what their government is doing, then some of the tools of power must be shared with the people, and that is the purpose of freedom of information legislation."[7]

Information commissioners appointed under the federal government's key information law, the *Access to Information Act* (*Access Act*), express similar views. The then information commissioner John Grace used colourful language to describe this perspective in his 1998 annual report:

> Any society aspiring to be free, just and civil must depend upon and nurture a wide array of methods for exposing, and imposing sanctions on, ethical failures...In one way or another, all the checks and balances designed to limit abuses of government power are dependent upon there being access by outsiders to governments' insider information...Yes, webs of intrigue are more easily woven in the dark; greed, misdeeds and honest mistakes are more easily hidden. A public service which holds tight to a culture of secrecy is a public service ripe for abuse. (Information Commissioner of Canada 1998, 4)

The courts have also recognized the importance of free access to information in a democracy. In his reasons in *Dagg v. Canada*, Justice La Forest urged that "the overarching purpose of access to information legislation...is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry."[8] While Justice La Forest was writing in dissent, his approach to interpreting the *Access Act* was endorsed by the majority in that case and has since been followed by the lower courts.[9]

More recently, the Supreme Court has noted that the *Access Act* makes information "equally available to each member of the public because it is thought that the availability of such information, as a general matter, is necessary to ensure the accountability of the state and to promote the capacity of the citizenry to participate in decision-making processes."[10]

Open government guarantees

As the discussion above suggests, the open government concept is protected at the federal level principally by the *Access Act*.[11] The *Access Act* creates a broad principle of access in its first dozen or so sections. It then devotes a sizeable portion of its remaining sections to the creation of exceptions and caveats to this principle.

The express purpose of the Act is "to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government" (section 2).

The key provision of the Act, section 4, provides that every Canadian citizen and permanent resident "has a right to and shall, on request, be given access to any record under the control of a government institution," subject to other sections in the Act.

Notably, the Federal Court has referred to this right as "quasi-constitutional" in nature.[12] In part, this status reflects language in subsection 4(1) specifying that the right in section 4 applies notwithstanding any other statute.[13]

The Act creates a mechanism for policing government decisions on disclosure and its use of exemptions. An office of the information commissioner is created and is charged with investigating access complaints brought by information requesters.[14] The commissioner – an officer of Parliament – has extensive powers to conduct investigations but has no power to compel the release of the information if he or she feels that such release is warranted. Instead, to compel disclosure, the information commissioner, or any requester dissatisfied with the outcome of the commissioner's investigation, must bring an application to the Federal Court.[15]

Open courts

The open court principle is tied to fair trials. Fair trial rights in international law require a presumptively open court.[16] In Canadian law also, court proceedings are presumptively open. The Supreme Court of Canada has repeatedly underscored this point,[17] pointing to the common law and relying on the Canadian Charter of Rights and Freedoms.[18] For instance, the Supreme Court has held that "freedom of expression in section 2(b) protects both listeners and readers."[19] It therefore supports open courts: "openness permits public access to information about the courts, which in turn permits the public to discuss and put forward opinions and criticisms of court practices and proceedings."[20]

Further, it is axiomatic in international[21] and Canadian criminal and constitutional law that the accused in criminal matters be given full disclosure of the state's evidence against them. Subject to legitimate exceptions for privileged evidence, the Crown in Canada has a legal duty to disclose its relevant evidence to the defence. As the Supreme Court of Canada noted in the leading authority on this point, *R. v. Stinchcombe*, "the right to make full answer and defence is one of the pillars of criminal justice on which we heavily depend to ensure that the innocent are not convicted. Recent events have demonstrated that the erosion of this right due to nondisclosure was an important factor in the conviction and incarceration of an innocent person."[22] As a consequence, the

> Crown obligation to disclose all relevant and non-privileged evidence, whether favourable or unfavourable, to the accused requires that the Crown exercise the utmost good faith in determining which information must be disclosed and in providing ongoing disclosure. Failure to comply with this initial and continuing obligation to disclose relevant and non-privileged evidence may result in a stay of proceedings or other redress against the Crown, and may constitute a serious breach of ethical standards.[23]

Read together, these rules create an open, transparent and fair system of adjudication. This openness is not absolute – it may be attenuated by rules on secrecy, not least in the *Canada Evidence Act* (*CEA*). But open courts and full disclosure are the starting point.

Indeed, the spirit – if not the specifics – of *Stinchcombe* now inform disclosure of security intelligence in proceedings that, while not criminal, place at risk Charter-protected interests in life, liberty and security of the person. In 2008, the Supreme Court held in *Charkaoui II* that full disclosure obligations applied in immigration security certificate proceedings and extended to material in the possession of CSIS. Here, "full" disclosure does not mean that this information will be passed to the person subject to the certificate – it may not be, because of secrecy concerns of the sort discussed below. However, at the very least, the full record must be disclosed to the judge and the special advocate, a special security-cleared lawyer representing the interests of the named person. Moreover, for this disclosure obligation to be realized, "CSIS officers must retain their operational notes when conducting investigations that are not of a general nature" – that is, "whenever CSIS conducts an investigation that targets a particular individual or group."[24]

Principles of National Security Confidentiality

The ambiguity of "national security"

The values reflected in the open court and open government concepts notwithstanding, national security imperatives may require limitations on both of these forms of transparency. Exactly when and to what extent secrecy is justified depends, however, on a sound understanding of "national security." No serious observer would advocate, for example, posting Canadian troop deployments in Afghanistan for the forthcoming week on the Internet. Other scenarios are, however, more fraught with ambiguity. Is national security imperilled, for example, by the release of Canadian government reports critical of conditions in the Afghan prisons to which the Canadian Forces transfer their battlefield detainees? There are a number of interests that might be prejudiced by the release of this prison report; not least, relations with the Afghan authorities embarrassed by a frank and damning report by their Canadian allies.

An injury to international relations should not be automatically conflated with an injury to national security, nor should it necessarily be given the same level of protection. Precluding embarrassment of a foreign government and the preservation of Canadian lives are on very different levels in terms of the justification for secrecy they create. The problem is, however, that "national security" defies clear definition and is therefore vulnerable to mutable and very elastic meanings. As noted in a 2002 IRPP study, "the term national security is used frequently to refer to matters ranging from domestic or internal security through to

international security, but is seldom defined" (Macnamara and Fitz Gerald 2002, 7). When some effort is made to set out its content, the definition is often so broad as to be meaningless. For instance, instructors at the National Defence College defined national security in 1980 as "the preservation of a way of life acceptable to the Canadian people and compatible with the needs and legitimate aspirations of others." National security, these authorities asserted, "includes freedom from military attack or coercion, freedom from internal subversion, and freedom from the erosion of the political, economic, and social values which are essential to the quality of life in Canada" (cited in Macnamara and Fitz Gerald, 8). As is immediately evident, this definition wraps much of what governments exist to do in a blanket of national security, a fact acknowledged even by those comfortable with this definition.[25]

The Government of Canada's April 2004 national security policy offers more recent and helpful guidance. That document describes national security as dealing "with threats that have the potential to undermine the security of the state or society" (Privy Council Office 2004, 3). The three specific threats the government seeks to address are: first, "protecting Canada and the safety and security of Canadians at home and abroad" (which includes "protecting the physical security of Canadians, our values, and our key institutions"); second, "ensuring that Canada is not a base for threats to our allies"; and, third, "contributing to international security" (5).

While this threat-based description of national security is narrower than the National Defence College version, it is still extremely general. Note especially the reference to the protection of "Canadian values" (whatever these may be) as a national security objective in the government's definition. Moreover, the description does little to define exactly when threats of the sort listed in the definition constitute national security concerns. As the 2004 policy acknowledges, most criminal offences threaten personal security but do not generally challenge the "security of the state or society." The policy does not answer the question, however, of when exactly a threat to the physical safety of Canadians becomes a legitimate national security concern rather than a regular policing matter, an uncertainty that has important implications when national security is invoked to justify secrecy.

The problem of ambiguity and imprecision is an acute one in the application of national security confidentiality. Not least, doctrines developed when Canada confronted a very different security threat – a Cold War adversary with a sophisticated intelligence-gathering capacity – have been deployed in a modern security context in relation to a much more inchoate (and almost certainly much less capable) adversary: terrorist groups.

It is possible, however, to extract from the 2004 policy a rough working definition of national security tied to the three threats that policy is designed to prevent. With this understanding in mind, justifications for national security confidentiality in Canada fall into two broad classes. First, there is information that, if released, could increase the likelihood of a threat to national security. Second, there is information that, if released, might cause injury to an intelligence relationship between Canada and allied states, whether or not it would also cause injury to a more specific Canadian national security objective.

Deterring a national security threat

There is no limit to specific threats to Canada, nor to the activities that might exacerbate these threats. I will, however, posit three obvious subclasses of national-security-related information, the revelation of which would likely enhance threats to the physical security of Canadians or of our allies, or undermine our contributions to international security: technology; plans and tactics; and sources and methods.

Technology

Certain technologies obviously provide advantages to those who possess them and constitute potential threats to those who do not. Preserving a technological advantage – and keeping potentially dangerous technologies out of the hands of adversaries – is a key and typically uncontroversial national security objective. At its core, technology is a manifestation of knowledge. Limiting access to technologies may mean restricting access to hardware, but it also means constraining the spread of technological know-how. Limiting the spread of technology may, therefore, require secrecy.

Plans and tactics

Adversaries gain advantage by knowing their opponents' plans or being able to predict those opponents' conduct accurately. Guarding plans of action and habits of conduct from adversaries is a core objective of national security confidentiality. Plans subject to such confidentiality could be, for example, deployment instructions to the Canadian Forces in Afghanistan, or the precise travel route of a visiting dignitary at poten-

tial risk of assassination. Tactical information, for its part, may include the doctrines that guide these decisions on deployment and travel planning for dignitaries. Open familiarity with these habits and patterns may allow predictions by adversaries that are almost as prejudicial as actual knowledge of specific plans.

Sources and methods

Information on government capabilities and capacities – especially in the sensitive areas of national defence and security and intelligence – is also closely guarded. An adversary who is intimately familiar, for example, with the technological abilities and limitations of Canada's signals intelligence agency, Communications Security Establishment Canada (CSEC), could employ this knowledge to circumvent detection. Likewise, an individual who is privy to the methodologies employed by CSIS in surveilling targets might rely on this knowledge to avoid monitoring. Indeed, chief among the cardinal secrets of any clandestine activity is the identity of informers, be they undercover agents or members of target communities or organizations.

Court jurisprudence gives some indication of the importance the security services place on protecting sources and methods. CSIS, for example, opposes disclosure of any information that may "identify or tend to identify":

> a) Service employees or internal procedures and administrative methodology of the Service, such as names and file numbers...
>
> b) investigative techniques and methods of operation utilized by the Service...
>
> c) Service interest in individuals, groups or issues, including the existence or absence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations...
>
> d) human sources of information for the Service or the content of information provided by a human source...
>
> e) relationships that the Service maintains with foreign security and intelligence agencies and would disclose information received in confidence from such sources; and...
>
> f) information concerning the telecommunication system utilized by the Service.[26]

Preserving international relationships

Canadian law often amalgamates justifications for secrecy predicated on national security and those associated with international affairs. However, confidentiality dictated by international relations preoccupations often has little to do with "national security" as the term is used in this paper. Canada's negotiating position at the World Trade Organization and in other treaty contexts is not, for instance, a matter of national security.

That said, there are instances where national security and international relations overlap. A dominant preoccupation for governments is guarding the secrets shared by allies. A failure to do so might prompt allied agencies to restrict their information sharing. As a middle power with limited foreign intelligence capacities, Canada is particularly dependent on information supplied by foreign intelligence services. It is, therefore, keenly aware of the need to observe so-called originator control rules. Originator control puts control over the use and distribution of the information in the hands of the state from which it comes. It is typically associated with the so-called third party rule, which bars the recipient of information from sharing it with a third party without the permission of the originating entity.

The third party rule is a regular fixture in the Canadian approach to national security confidentiality. Originator control provisions are likely commonplace in international information-sharing agreements. CSIS told a Federal Court in 1996 that the information it receives is "invariably provided in confidence and on the explicit or implicit understanding that neither the information nor its source will be disclosed without the prior consent of the entity which provided it."[27] This principle is "widely recognized within the policing and security intelligence communities,"[28] an observation confirmed by RCMP, Department of National Defence (DND) and Department of Foreign Affairs and International Trade (DFAIT) submissions in the same case.

CSIS told the same court that "CSIS receives sensitive information, not just because of the third party rule which requires CSIS to treat the information as confidential, but also because there is confidence on the part of information providers that the Canadian government understands the need for confidentiality and has in place practices and procedures to safeguard information."[29] Without this confidence in Canada's ability to restrict disclosure, some allies "may discontinue the alliance or association. Others may continue their alliance, but with a reluctance to be candid."[30] Similar views were expressed in this and other cases[31] by the RCMP, DND and DFAIT. The RCMP – which reports that it receives 75 times more information from partner agencies than it provides – applies third-party-rule limitations even when documents do not contain emphatic constraints on sharing information with third parties.[32]

The current security focus on counterterrorism has, if anything, augmented international intelligence flows, and therefore the potential application of the third party rule. The director of operations of CSIS described the environment for information sharing this way in 2004: "compromising al-Qaeda operatives requires an unprecedented level...of cooperation between police, law enforcement, and immigration officials and the like, not just domestically but internationally as well."[13] As the Arar Commission report later noted,

> Information sharing among agencies allows a more comprehensive picture to emerge. Viewing different pieces of information together may allow a more complete and accurate assessment of the threat being investigated and the steps needed to address that threat. Sometimes, seemingly inconsequential bits of information may take on an importance not otherwise apparent when viewed alongside other information. Broad information sharing is therefore essential to effective prevention. (Commission of Inquiry 2006, 102)

More generally, intelligence sharing permits the "acquisition of intelligence that is valuable to decision makers but otherwise unobtainable at an acceptable cost" (Walsh 2007, 157). As such, it is particularly important for small countries like Canada to be able to use alliance relationships to tap into the intelligence capacities of larger states. Intelligence sharing is, however, also vital for larger states, including the United States. In 1985, then defense secretary Caspar Weinberger observed that the "United States has neither the opportunity nor the resources to unilaterally collect all the intelligence information we require. We compensate with a variety of intelligence sharing arrangements with other nations in the world."[14] The more recent focus on terrorism has likely compounded this US dependency on foreign information sharing. In the words of one commentator, writing about terrorism:

> the point of impact is not necessarily the same as the point of origin. Therefore, in order for an individual state to make a meaningful assessment of its security situation it needs to process information pertaining to individuals and events existing in far-off places at any given time. No single state has the power to collect and exploit this type and volume of information; intelligence sharing between states has become essential even from the perspective of the most powerful intelligence producers, such as the US. (Mackmurdo 2007, 207)

Legal protections for national-security-related information

The objectives of national security confidentiality set out above are largely unassailable and self-evident. The implementation of these objectives in Canadian law and policy is much more complex. Discerning whether the interests discussed above are truly engaged, and whether they are engaged to a degree that justifies secrecy, is a matter of judgment. How that judgment may be deployed is ultimately a matter set down in law. National-security-related information is protected at several levels in Canadian information law: laws limiting open government rules otherwise applicable to the executive branch; laws that constrain the open court concept and disclosure rules typically applied by Canada's courts; and statutes that criminalize the wrongful disclosure of particularly sensitive information.

Limiting open government

By 2006, 68 states had enacted access to information laws (Banisar 2006). The right to information is not absolute; nearly all of these laws include common exceptions relating, *inter alia*, to national security and international affairs and the protection of information obtained in confidence from other states (Banisar 2006, 22).

Canada is no different in this respect. While principally an information disclosure law, the *Access Act* includes important limitations on open government, several of which are tied to national security.[15] These constraints include exemptions, that is, excuses for redacting sensitive information from released records, and a new national security exclusion – a blanket override of the *Access Act* and its mechanisms.

The exemptions are of venerable vintage, mostly unchanged from the time the *Access Act* was enacted, in the early 1980s. They are reasonably precise in their drafting, although they are not without inherent ambiguity. In comparison, the exclusion was enacted in haste in 2001 in the immediate aftermath of 9/11. It is not so carefully considered or drafted.

National security exceptions

The *Access Act*'s national-security-related exemptions are summarized in table 1. These exemptions can be categorized in two ways: injury-based/class-based exemptions and mandatory/discretionary exemptions.

Injury-based exemptions may be employed only where the government concludes that disclosure may produce the harm enumerated by the Act.[16] By comparison, class-based exemptions are triggered as soon as the information requested is found to fall within a certain

class of information, as defined by the Act. Put another way, the exemption is triggered by the type of information at issue, without any consideration of whether disclosure of that information would actually be "injurious" to some listed government interest. This gives class-based exceptions a broad reach.

In the national security area, all the class-based exceptions are also mandatory. With mandatory exemptions, the government is obliged to decline disclosure once the information falls within the class of protected data, subject in a few instances to a public interest override. Mandatory class-based exceptions are the most robust secrecy protection offered by the *Access Act*. No doubt for exactly this reason, information received in confidence from other governments falls within this category.

In fact, however, the majority of exceptions in the Act are not mandatory, but rather discretionary. Thus, the government *may* (but need not) choose to decline disclosure of a document captured by the exemption.

Turning to specific examples, section 16(1)(a) and section 15 of the *Access Act* are the most obvious national-security-related exceptions.

Information pertaining to threats to the security of Canada Section 16(1)(a) allows the government to refuse release of requested records less than 20 years old that contain information prepared by a government investigative body in the course of lawful investigations of activities suspected of constituting "threats to the security of Canada" within the meaning of the *Canadian Security Intelligence Service Act* (*CSIS Act*).[37] The latter concept is carefully defined, although in a manner that creates ambiguity of its own.

The formulation and inclusion of the concept of "threats to the security of Canada" was the subject of sustained discussion at the time Parliament enacted the *CSIS Act*, in 1984. It has also drawn the attention of the review agency empowered to scrutinize CSIS's activities, the Security Intelligence Review Committee (SIRC). In one of its early reports of CSIS, the SIRC questioned several aspects of the threat definition in the Act. These concerns are summarized in table 2.

Even with these shortcomings, however, the definition of "threats to the security of Canada" is robust when compared to the looser invocations of "national security" that have figured in more recent laws.

Table 1
National Security Exemptions in the *Access to Information Act*

	Class-based exemptions	Injury-based exemptions
Mandatory exemptions	• Section 13 – Information received in confidence from other governments or an international organization, if the body gives disclosure permission (or this body has itself made public the information), the information may be disclosed • Section 20 – Information supplied in confidence by third parties concerning emergency management plans relating to the vulnerability of critical infrastructure, subject to a public interest override • Section 24 – Information protected under other, listed statutes	
Discretionary exemptions	• Paragraph 16(1)(a) – Information obtained or prepared by listed investigative bodies pertaining to crime prevention, law enforcement or threats to the security of Canada, if less than 20 years old • Paragraph 16(1)(b) – Information on techniques or plans for specific lawful investigations	• Section 15 – Information that could reasonably be expected to be injurious to the conduct of international affairs or to the defence of Canada or an allied state, or the prevention or suppression of subversive or hostile activities • Paragraph 16(1)(c) – Information that could reasonably be expected to be injurious to law enforcement or to the conduct of lawful investigations, including information on confidential sources • Paragraph 16(1)(d) – Information that could reasonably be expected to be injurious to the security of penal institutions • Subsection 16(2) – Information that could reasonably be expected to facilitate the commission of an offence, including technical information relating to weapons or potential weapons or information on the vulnerability of particular buildings or other structures or systems • Section 17 – Information the disclosure of which could reasonably be expected to threaten the safety of individuals

Table 2
Definitions of "Threats to the Security of Canada"

Type of threat	Definitions in the *CSIS Act*	Critique by the Security Intelligence Review Committee[1]	CSIS interpretation[2]
Espionage and sabotage	"Espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage."	"*Detrimental to the interests of Canada*": The phase is "wholly subjective" as "no criteria are provided to offer any standard for determining what is 'detrimental.'" It should, therefore, be defined in the Act.	*Espionage*: "Activities conducted for the purpose of acquiring by unlawful or unauthorized means information or assets relating to sensitive political, economic, scientific or military matters, or for the purpose of their unauthorized communication to a foreign state or foreign political organization." *Sabotage*: "Activities conducted for the purpose of endangering the safety, security or defence of vital public or private property, such as installations, structures, equipment or systems."
Foreign-influenced activities	"Foreign-influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."	"*Foreign influenced*": The phrase "foreign influenced" is broad, covering "foreign interest groups, political organizations, individuals, associations and corporations," while the concept of "influenced" is ambiguous and should be replaced with "directed." "*Within or relating to Canada*": "There are no criteria set out in the Act to help determine how much any particular activity must 'relate' to Canada before CSIS can take jurisdiction, creating a requirement that may be too easily met." "*Clandestine or deceptive*": "The precise meaning of the term 'clandestine' is uncertain. It may connote an element of underhandedness or male fides, but some dictionary definitions would support an interpretation that merely 'secret' activities may be 'clandestine'. The term should be replaced with a word like 'surreptitious,' which more clearly connotes some element of underhanded behaviour." "*Detrimental to the interests of Canada*": The phrase is "wholly subjective" as "no criteria are provided to offer any standard for determining what is 'detrimental.'" It should, therefore, be defined in the Act. "*Involve a threat to any person*": The term "threat" should be modified by an adjective like "serious."	"Activities detrimental to the interests of Canada, and which are directed, controlled, financed or otherwise significantly affected by a foreign state or organization, their agents or others working on their behalf."
Political violence and terrorism	"Activities within or relating to Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state."	"*Political, religious or ideological objective*": The reference to "political, religious or ideological objective" was added to the *CSIS Act* by the 2001 *Anti-terrorism Act*. The phrase "political, religious or ideological objective" when used in the context of the Criminal Code's definition of "terrorist activity" was declared unconstitutional by a lower court in 2006. In the wake of that decision, jurists speculated that the equivalent phrase in the *CSIS Act* might render information collected by CSIS constitutionally suspect, if employed in a subsequent criminal prosecution.[4] To minimize the prospect of ethnic profiling, the special Senate committee on antiterrorism law recommended its repeal in its 2007 report.[5]	"Threat or acts of serious violence may constitute attempts at compelling the Canadian government to respond in a certain way. Acts of serious violence cause grave bodily harm or death to persons, or serious damage to or the destruction of public or private property, and are contrary to Canadian law or would be if committed in Canada."
Subversion	"Activities directed towards undermining by covert unlawful acts, or directed towards or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada."	SIRC recommended repeal of this provision, urging that it presented the greatest risk in a democracy and that its core content – avoiding political violence – is already covered in the other paragraphs.	"Activities intended to undermine or overthrow Canada's constitutionally established system of government by violence. Subversive activities seek to interfere with or ultimately destroy the electoral, legislative, executive, administrative or judicial processes or institutions of Canada."

[1] Unless otherwise noted, these critiques are drawn from Security Intelligence Review Committee (SIRC) (1989).
[2] Extracts cited in this column drawn from Canadian Security Intelligence Service (2005).
[3] S.C. 2001, c. 41.
[4] See discussion in MacLeod (2006).
[5] Special Senate Committee on the *Anti-terrorism Act* (2007, 20).

Conduct of international affairs, defence or the prevention of subversion Under section 15 – an exception whose equivalent in the *Privacy Act* the Supreme Court of Canada has labelled a "national security"[38] exemption – the government may refuse to disclose any record requested under the Act "that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities."[39]

While "international affairs" is not defined, the expression "defence of Canada or any state allied or associated with Canada" is limited to efforts by Canada and foreign states "toward the detection, prevention or suppression of activities of any foreign state directed toward actual or potential attack or other acts of aggression against Canada or any state allied or associated with Canada."[40] Meanwhile, the expression "subversive or hostile activities" is also carefully delimited.[41]

National security exclusion

Read together, the *Access Act* exemptions provide government with substantial power to shield national security secrets from the effects of the Act. It is notable that the security and intelligence community itself apparently had few quibbles with the scope of the *Access Act* exemptions. In an admittedly now dated and pre-9/11 study prepared for the government's Access to Information Review Task Force, Wesley Wark reported that "both the Canadian Security and Intelligence Service and the Communications Security Establishment, the two main collectors of sensitive intelligence in the community, regard the Access Act as offering sufficient protection." Given the breadth of these exemptions, Wark labels access to contemporary intelligence records under the Act "a fiction," and concludes that "the current Access exemptions provide powerful and sufficient tools" for protecting intelligence information (2001, section 2).

Yet, notwithstanding the breadth of long-standing Canadian exemptions from Canada's access statutes, the government moved to enhance its power to keep information secret in its 2001 *Anti-terrorism Act* (*ATA*).[42] Specifically, since 2001, the *CEA*[43] now has a central place in government secrecy law.

***Canada Evidence Act* amendments** The *CEA*'s primary purpose is to set out several evidentiary standards for "proceedings."[44] Among its provisions are special rules limiting access to certain sensitive information during these proceedings. For the most part, the decision on whether to disclose this sensitive information is in the hands of the Federal Court. However, the Act empowers the attorney general to issue a certificate "in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security."[45]

The minister's certificate decision may be challenged in only a perfunctory manner, before a single judge of the Federal Court of Appeal. The role of this judge is simply to determine that the information covered by the certificate "relates to" the permissible grounds for issuing a certificate, in which case the judge must confirm the certificate.[46] The concept of "relates to" is ambiguous. Indeed, in 2007, a special Senate committee examining antiterrorism law recommended that the Act be amended to "specify the way in which information must 'relate to' information obtained in confidence from a foreign entity, or to national defence or national security, in order for that aspect of the certificate to be confirmed by a judge" (Special Senate Committee on the *Anti-terrorism Act* 2007, 65), and that the judge be empowered to consider "whether the public interest in disclosure outweighs in importance the public interest in non-disclosure" (67).

Implications for the *Access Act* Although these powers have not yet been used, amendments introduced to the *Access Act* by the *ATA* give attorney general's certificates clear primacy over the right to access. They do so by creating a new exclusion. Section 69.1 now specifies that the *Access Act* "does not apply" to information covered by a *CEA* certificate issued before an access complaint is filed with the information commissioner and, if issued after a complaint, quashes all proceedings in relation to that complaint.[47] The effect of a certificate is, therefore, to preclude release of the information and deny the information commissioner a role in assessing whether nondisclosure is warranted.

Limiting open courts

As discussed above, the Canadian judicial system guarantees open and transparent adjudication of disputes in the form of open courts – with ready access to the information at issue in them – and full disclosure to litigants, especially the accused in criminal matters. National security does not negate either the

open court principle or rules on disclosure. It may, however, limit the reach of these doctrines.

Notably, the potential conflict between national security confidentiality and the open court principle has become more acute in the last several years, as the dominant focus of security intelligence has shifted from the actions of sovereign states to an era of counterterrorism. The intelligence activities required to combat the interests of potential state adversaries are very different from those associated with countering a diffuse, more autonomous and more individualized terrorist movement. Counterintelligence against states occurs within the broader envelope of international relations; not least, foreign state agents may be accredited diplomats, and those exposed as spies are expelled rather than prosecuted.

Terrorists are, first and foremost, criminals, and unless a state is prepared to take extralegal action against them, the response to terrorists among the populace is a criminal law one, as bolstered by administrative law mechanisms like immigration proceedings. Legal responses require appropriate regard for due process, which ensnares intelligence agencies in a judicial process to which they are unaccustomed, producing what CSIS director Jim Judd has called the "judicialization" of intelligence (2008). The net result is acute tensions between the classic secrecy doctrines of the intelligence world and the overt transparency of the judicial process.

Closing courts for national security reasons

In *Re Vancouver Sun*, the Supreme Court observed that even in national security matters "the open court principle is a fundamental characteristic of judicial proceedings, and that it should not be presumptively displaced in favour of an *in camera* process."[48] The question of closed proceedings must be left in the hands of judges, not mandated in advance by statute. Further, where judges exercise that discretion, they must balance the national security impulse against the public interest in openness, and not simply give primacy to one principle over the other. A constitutional doctrine, this approach has been "read into" several existing statutory rules for closing courts on national security grounds.[49]

Limiting disclosure of evidence for national security reasons

Restrictions on full disclosure of information by the government to other parties in court proceedings are also permissible in Canada. These rules on secret evidence are summarized in table 3.

The *Canada Evidence Act* The *Canada Evidence Act (CEA)* is the most important statute governing secrecy in court proceedings. Amendments made by the 2001 *ATA* to section 38 of the *CEA* contain special rules limiting access to "potentially injurious information" and "sensitive information" in "proceedings," including criminal trials.[50]

The concepts of potentially injurious information and sensitive information are broadly defined: potentially injurious information means "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security," whereas sensitive information means "information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard."[51] As this language suggests, sensitive information need not be of a sort that if released could cause injury; it must merely "relate to" international relations, national defence or security.[52]

Participants in a proceeding must notify the attorney general when they intend (or believe another participant or person intends) to disclose these classes of information. The attorney general may then authorize disclosure or, alternatively, may deny this authorization, in which case the matter is taken up by the Federal Court.

In adjudicating the section 38 dispute, the Federal Court proceeds in three steps: first, it assesses whether the evidence is relevant to the proceeding in question; second, it determines whether disclosure would be injurious to international relations, national defence or national security; and third, it determines whether the public interest in disclosure outweighs the public interest in nondisclosure.[53] At the end of this process, the judge may authorize disclosure (or not).

However, as already noted, the *CEA* allows the government to short-circuit a court disclosure order. The attorney general may issue a certificate "in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security."[54] Issuance of the certificate has the effect of barring any subsequent disclosure of the information in a proceeding for 15 years (and for a further period if the certificate is renewed at the end of that 15 years). In other words, the certificate may reverse an order from the Federal Court authorizing

Table 3
Secret Evidence Rules in Canadian Law

Context	Basis	Application	Scope	Limitation
Informer privilege	Common law	Typically criminal proceedings	The informer privilege rule "prevents not only disclosure of the name of the informant, but of any information which might implicitly reveal his or her identity."[2]	Informer privilege is subject to the "innocence at stake" exception; that is, secrecy will give way where "disclosure of the informer's identity is necessary to demonstrate the innocence of the accused."[1] Where informer privilege yields to the innocence at stake doctrine, "the State then generally provides for the protection of the informer through various safety programs."[3]
Section 38	*Canada Evidence Act*	All "proceedings," including criminal trials[4]	Allows government to refuse disclosure of "potentially injurious" and "sensitive" information.	A federal court judge decides whether the public interest in disclosure outweighs the public interest in nondisclosure
Security certificates	*Immigration and Refugee Protection Act*	Immigration proceedings in which the government issues a security certificate (as well as a possible use in regular removal proceedings)[5]	A judge may refuse to disclose anything that, in the judge's opinion, would be injurious to national security or endanger the safety of any person if disclosed.	The interests of persons subject to security certificates are now defended by "special advocates" entitled to see all the evidence, but who may only have limited communication with the person whose interest they are defending.[5]
Terrorist group listing	Criminal Code	Listing of groups as "terrorist groups" under the Criminal Code,[6] appealable before a judge.	A judge may, at the request of the attorney general, hear all or part of the government's evidence or information in the absence of the applicant and any counsel representing the applicant, "if the judge is of the opinion that the disclosure of the information would injure national security or endanger the safety of any person."[7]	The judge must provide a summary of the confidential information.
Terrorist-financing certificate	*Charities Registration (Security Information) Act*	Issuance of a certificate attesting that a charity (or applicant for charitable status) is involved in terrorist financing, adjudicated before a judge	See entry for "Terrorist group listing" above.[8]	The judge must provide a summary of the confidential information.[9]
Terrorism-financing regulations	*United Nations Act*	Listing of a person believed to be affiliated or associated with terrorist activity, appealable before a judge	See entry for "Terrorist group listing" above.	Same as terrorist group listing process above.

[1] *R. v. Leipert*, [1997] 1 S.C.R. 281 at para. 21.
[2] *Ibid.* at para. 18.
[3] *R. v. McClure*, 2001 S.C.C. 14 at para. 45.
[4] *Canada Evidence Act*, s. 38. For a discussion of the scope of s. 38 in relation to the earlier doctrine of "public interest immunity," see Stewart (2003).
[5] *Immigration Refugee Protection Act*, s. 83(1)(e).
[6] Criminal Code, s. 83.05.
[7] Criminal Code, para. 83.05(6)(a).
[8] *Charities Registration (Security Information) Act*, S.C. 2001, c. 41, s. 113, s.6.
[9] Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360, s.2.2.

disclosure, subject to a limited appeal before a single judge of the Federal Court of Appeal.[55]

The system established by the Act would be vulnerable to constitutional attack in those circumstances where a person's innocence in a criminal trial can only be proven by evidence that the Federal Court refused to disclose, or that is subject to an attorney general's certificate barring that disclosure. To compel trials to proceed even where the only evidence available to establish the accused's innocence is withheld from him or her would be an unquestionable violation of section 7 of the Charter of Rights and Freedoms.[56]

The Act sidesteps this possible clash between legal rights and the state's secrecy preoccupation by providing criminal trial judges with an escape from the dilemma:

> The person presiding at a criminal proceeding may make any order that he or she considers appropriate in the circumstances to protect the right of the accused to a fair trial, [other than ignoring a Federal Court determination on disclosure or a Attorney General's certificate].
>
> Among the permissible orders are those:
>
> (a) dismissing specified counts of the indictment or information, or permitting the indictment or information to proceed only in respect of a lesser or included offence...
>
> (b) effecting a stay of the proceedings and...
>
> (c) finding against any party on any issue relating to information the disclosure of which is prohibited.[57]

Immigration proceedings The *CEA* process is quite different from that applied in the controversial immigration security certificate process under the *Immigration Refugee Protection Act* (*IRPA*).[58] That process allows the government to issue a certificate against a foreign national or permanent resident, seeking that person's removal (and detention pending removal) on national security grounds, among other things. The reasonableness of this certificate (and the duration of any detention pending removal) is adjudicated before a Federal Court judge. The government is entitled, however, to present information to that judge in closed sessions and without the person subject to the certificate (and his or her lawyer) being present. Moreover, the person receives only a summary of this secret information, sometimes of the most general sort.[59]

The criterion for what is released is based exclusively on the national security (or public safety) preoccupation: in providing the summary,

> the judge shall ensure that the permanent resident or foreign national is provided with a summary of information and other evidence that enables them to be reasonably informed of the case made by the Minister in the proceeding but that does not include anything that, in the judge's opinion, *would be injurious to national security or endanger the safety of any person if disclosed*. [emphasis added][60]

Unlike the *CEA*, under the *IRPA* there is no balancing of the secrecy interest against the fair trial imperative. Nor is there any fair trial protection (also present in the *CEA*) authorizing a judge to throw out the government case if disclosure to the interested person is insufficient to meet basic fairness expectations.

The security certificate process obviously constrains the interested person's ability to meet the case against him or her; the information that is provided is often so oblique as to be useless in understanding the government's case. This problem becomes acute – and indeed a constitutional matter – when the risk to the interested person is taken into account: detentions under security certificates have been lengthy,[61] and several of the most recent cases have involved individuals said to present terrorist threats who may well be tortured (or worse) if returned to their countries of origin.

In its 2007 *Charkaoui* decision,[62] the Supreme Court concluded that the secrecy in the security certificate process violated the Charter, underscoring that "before the state can detain people for significant periods of time, it must accord them a fair judicial process."[63] In particular, the "magistrate must make a decision based on the facts and the law"[64] and "the affected person be informed of the case against him or her and be permitted to respond to that case."[65] The Court proposed a special counsel model as a possible solution to the conundrum of national security confidentiality and fairness in security certificate proceedings.

Criminalizing wrongful disclosure

The constraints on open government and open courts described to this point limit what information may be disclosed on national security grounds under rules favouring full disclosure. A third plank in Canada's national security information law relates to punishing those who wrongfully release (and potentially receive) sensitive information. To grapple with this prospect, Canadian law includes a number of information disclosure offences. First, it criminalizes unauthorized disclosure of sensitive information. Second, it proscribes physical spying – that is, the physical infiltration of sensitive locations. The *SOIA*[66] is the key statute creating both of these types of offence. In this paper I focus on its first objective – criminalizing unauthorized disclosure.

Background to the Security of Information Act

Originally enacted in 1939 as the *Official Secrets Act*,[67] the *SOIA* was substantially amended and renamed in December 2001, as part of the *ATA*. The 1939 Act was a variant on the United Kingdom's 1889 *Official Secrets Act*, and it had two main focuses. First, in section 3, it made espionage or spying an offence, and second, in section 4, it criminalized wrongful dissemination of information, sometimes called "leakage" (Canadian Security Intelligence Service 2004).

From the 1960s or earlier, this wartime statute was roundly condemned for its breadth and ambiguity. The 1969 report of the Royal Commission on Security (the Mackenzie Commission) called the 1939 law "an unwieldy statute, couched in very broad and ambiguous language"

(1969, para. 204). In 1986, the Law Reform Commission condemned the statute as "one of the poorest examples of legislative drafting in the statute books" (Law Reform Commission of Canada 1986, 30). It called the *Official Secrets Act* and other laws that criminalized "crimes against the state" as "out of date, complex, repetitive, vague, inconsistent, lacking in principle and over-inclusive," as well as potentially unconstitutional under the Charter of Rights and Freedoms (38-9).

In particular, the commission took issue with section 3 of the Act, relating to spying, which could be interpreted as imposing an onus of proving innocence on the accused. This reverse onus, the commission speculated, was inconsistent with subsection 11(d) of the Charter, which guarantees the presumption of innocence until proven guilty (39). The government itself criticized the statute in 1998, when the then solicitor general called the Act "badly outdated and overbroad."[68]

Perhaps for these reasons, the *Official Secrets Act* has rarely been invoked. CSIS reports that since 1939 there have been two dozen prosecutions under the Act, but only six in the past 40 years (2004). In one of these cases, Stephen Ratkai pleaded guilty in 1989 to charges under the espionage provisions of the statute for spying for the USSR. In sentencing Ratkai to two concurrent terms of nine years, the court commented that the object of the *Official Secrets Act* is "to protect the safety and interests of the state. Every country has an obligation to protect its citizens and its territory and countries must depend and rely upon its citizens to ensure [their] safety and security. What is disturbing and despicable about offences of this nature is that a citizen betrays his country which he has a duty to protect and defend."[69]

However, in *R. v. Toronto Sun* – probably the leading case on the *Official Secrets Act* – the court was moved much less by the Act's objectives than by its awkward structure. At issue in this pre-Charter case was whether a newspaper and its editors had violated the Act by printing excerpts of a top secret document about Soviet intelligence activities in Canada. The court concluded that they had not, as the allegedly secret information had already been invoked in the public domain. However, the court was also critical of the Act itself. In the court's words,

> since the Official Secrets Act is a restricting statute, and seeks to curb basic freedoms, such as freedom of speech and the press, it should be given strict interpretation...The statute must, in clear and unambiguous language, articulate the restriction it intends to impose upon a citizen. A reading of ss.3 and 4 of the Official Secrets Act amply demonstrates its failure to do so; the provisions are ambiguous and unwieldy...A complete redrafting of the Canadian Official Secrets Act seems appropriate and necessary.[70]

Unauthorized disclosure

In fact, the *ATA* subsequently repealed and replaced the much-criticized 1939 espionage provision. The current *SOIA* now includes a list of offences under the heading "Special Operational Information and Persons Permanently Bound to Secrecy." Most notably, persons employed at a number of security and intelligence government agencies are deemed (or are named by the government as) permanently bound to secrecy.[71] As table 4 suggests, these persons are criminally liable for the communication of "special operational information" subject to a public interest defence in limited circumstances. "Special operational information" is defined as and basically means military- and intelligence-related information that the government seeks to "safeguard."[72] The 2001 changes also introduced other provisions, governing other, more specific forms of unauthorized disclosure. These *SOIA* provisions supplement sections of the *CSIS Act* that criminalize unauthorized disclosure of information from which the identity of any CSIS informant or operative may be discerned. These offences are summarized in table 4.[73]

The new *SOIA* provisions might reasonably be critiqued for the breadth and uncertainty of the "special operational information" concept. At least, however, there is a definition – something notable for its absence in the section 4 antileakage provision. Most critically, the public interest override is an important feature, allowing secrecy to give way in exigent circumstances. Still, that override deserves renovation: except where necessary to avoid grievous bodily harm, the public interest defence exists only when two prerequisites are met. First, prior to disclosure, the whistle-blower must have provided all relevant information to his or her deputy head or the deputy attorney general of Canada and have received no response within a reasonable time. Subsequently, the whistle-blower must have also provided the information to the SIRC or, where the alleged offence concerns the CSEC, to the CSE commissioner, and must have not received a response within a reasonable time.

The Act leaves open the question of what would constitute a "reasonable time." Likewise, it does not

Table 4
Information Offences under the *Security of Information Act (SOIA)* and the *CSIS Act*

Type of information	Person to whom prohibition applies	Prohibition in the offence
"Special operational information"	Persons permanently bound by secrecy	Intentionally and without authority communicates or confirms information that, if it were true, would be special operational information (*SOIA*, s. 13)
		Intentionally and without authority communicates or confirms special operational information (*SOIA*, s. 14)
	Every person	Intentionally and without lawful authority communicates special operational information to a foreign entity or to a terrorist group if the person believes (or is reckless as to whether) the information is special operational information (*SOIA*, s. 17)
Information the government is "taking measures to safeguard"	Every person with a security clearance given by the Government of Canada	Intentionally and without lawful authority communicates, or agrees to communicate, to a foreign entity or terrorist group any information that is of a type that the Government of Canada is taking measures to safeguard (*SOIA*, s. 18)
	Every person	Without lawful authority communicates to a foreign entity or terrorist group information while believing (or reckless as to whether) that information is safeguarded and in order to increase the capacity of that foreign entity or terrorist group to do harm to Canadian interests (*SOIA*, s. 16)
		Without lawful authority communicates to a foreign entity or to a terrorist group information while believing (or reckless as to whether) that information is safeguarded, and harm to Canadian interests results (*SOIA*, s. 16)
Any information obtained or accessed in the course of the performance of duties and functions under this *CSIS Act* or participation in the administration or enforcement of the Act	Every person	Discloses this information and from it the identity of "(a) any other person who is or was a confidential source of information or assistance to the Service," or "(b) any person who is or was an employee engaged in covert operational activities of the Service" can be inferred (*CSIS Act*, s. 18)
Trade secrets	Every person	At the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right, communicates a trade secret to another person or organization or obtains, retains, alters or destroys a trade secret "to the detriment of" Canada's economic interests, international relations or national defence or national security[1]

[1] The economic espionage offence in section 19 is constrained in subsection 19(3) by certain defences protecting independent development of trade secrets or reverse engineering.

address whether the public interest defence would apply were the responses received from these review bodies inadequate. Indeed, it does not spell out exactly how the review bodies are to respond to the disclosures, a point made by the Special Senate Committee on the *Anti-terrorism Act* in 2007.

Criminalized leakage

The *ATA* was notable as much for what it did *not* do as for what it changed in *SOIA*. The 2001 amendments left intact section 4, criminalizing leakage; that is, the simple unauthorized disclosure (or, in some cases, receipt) of secret (or sometimes merely official) information. This omission provoked substantial controversy soon afterward.

Criticisms of the leakage provision As with the now repealed section 3, dealing with espionage, the precise scope of section 4 of the 1939 *Official Secrets Act* is difficult to discern from the drafting of the section itself. In *Keable v. Canada (Attorney-General)*,[74] the Supreme Court held that "Section 4 of the *Official Secrets Act* makes it clear that it is the duty of every person who has in his possession information entrusted in confidence by a government official and subject to the Act, to refrain from communicating it to any unauthorized person."

Table 5
The Leakage Provision in Section 4 of the *Security of Information Act (SOIA)*

Type of information	Person to whom prohibition applies	Prohibition in the offence
Any secret official code word, password, sketch, plan, model, article, note, document or information that relates to or is used in a prohibited place	Every person in possession	• Fails "to take reasonable care of," or endangers the "safety of" the information (*SOIA*, para. 4[1][d])[1] • Communicates the information "to any person, other than a person to whom he [or she] is authorized to communicate with, or a person to whom it is in the interest of the State his [or her] duty to communicate it" (*SOIA*, para. 47[1][a]) • Uses the information "for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the State" (*SOIA*, para. 4[1][b]) • Retains the information in the absence of a "right to retain it or when it is contrary to [the receiving person's] duty to retain it or [he or she] fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof" (*SOIA*, para. 4[1][c])
Any secret official code word, password, sketch, plan, model, article, note, document or information	Every person receiving this information	Knows, or has reasonable ground to believe, at the time he or she receives it, that the information is communicated to him or her in contravention of this act, unless he or she proves that the communication of the information was contrary to his or her desire (*SOIA*, subs. 4[3])
Any sketch, plan, model, article, note, document or information that relates to munitions of war	Every person in possession	Communicates the information to "any foreign power" or "in any other manner prejudicial to the safety or interests of the State" (*SOIA*, subs. 4[2])
Any official document	• Person for whose use the information was issued • Every person	• Allows any other person to have possession of the document (*SOIA*, para. 4[4][b]) • Has possession "without lawful authority or excuse" of "any official document...issued for the use of a person other than" him or herself (*SOIA*, para. 4[4][b]) • Upon "obtaining possession of any official document by finding or otherwise," fails to "restore it to the person or authority by whom or for whose use it was issued, or to a police constable" (*SOIA*, para. 4[4][b]) • Retains "for any purpose prejudicial to the safety or interests of the State" an "official document, whether or not completed or issued for use, when he has no right to retain it, or when it is contrary to his duty to retain it" or in contravention of instructions from the government to return or dispose of it (*SOIA*, para. 4[4][a])

However, the section is much broader in scope than this interpretation suggests.

Indeed, communication of information is criminalized in a fashion likely to render most public service whistle blowing a crime. As the Law Reform Commission noted in 1986, the *Official Secrets Act* "always treats the loquacious public servant and the secret agent alike: both may be charged under the same section (section 4), the punishment is the same, and, more importantly, the terrible stigma of prosecution under the [Act] is identical for both, because the public and the news media are unable to discern whether it is a case of calculated espionage or careless retention of documents" (1986, 37).

So broadly crafted is section 4 of the *SOIA* that it was difficult to imagine that the government would, for example, fail to secure convictions for the almost daily "leaks" of written government information that fill newspaper pages. More than that, it seems likely that it could be used to secure the conviction of the journalists and newspapers reporting these leaks. The precise parameters of section 4 are set out in table 5.

Constitutionality of the leakage provision The historical absence of prosecutions brought under section 4 of the *SOIA* likely reflected a sober appreciation of the political consequences flowing from aggressive uses of secrecy law, coupled with a principled realization by prosecutors and others that the section was unusable. However, a law of this breadth could be used to either threaten a prosecution or obtain warrants, both of which are tactics that raise civil liberties issues. Most notoriously, in January 2004, the RCMP raided *Ottawa Citizen* reporter Juliet O'Neill's home and office looking for leaked information pertaining to Maher Arar, the Canadian deported by US officials to Jordan and then incarcerated and tortured in Syria. The warrant alleged a violation by O'Neill of section 4 of the *SOIA*.

That warrant, and the resulting search of O'Neill's home and office, sparked a constitutional challenge to section 4. Specifically, O'Neill and the *Ottawa Citizen* contended that section 4 violated section 2(b) of the Charter by infringing on the freedom of the press to gather and disseminate information of public interest and concern, and it contravened section 7 of the Charter on the basis of vagueness and overbreadth. Those claims were accepted by the Ontario Superior Court of Justice in 2006,[75] a decision the government chose not to appeal. Section 4 was also critiqued by the Special Senate Committee on the *Anti-terrorism Act* in 2007 (94ff). That body urged much clearer definitions of the information protected by the section and a public interest override where the public interest in disclosure exceeds the public interest in nondisclosure.

As it stands, the 2006 Ontario Superior Court of Justice decision remains the final word on section 4. It is critical to note, however, that this decision comes from a single lower court in one province. It would undoubtedly be considered by other such lower courts, were they presented with a question about the constitutionality of section 4. However, in Canada's common law system, the 2006 decision has no binding precedential effect. It could be rejected by another lower court, or by an appeal court. Put another way, section 4 lurks on the statute books and remains potentially of force and effect in any court other than the one that decided the Juliet O'Neill case.

Reconciling Transparency and National Security Confidentiality

I now turn to assessing how well Canadian law and practice reconcile transparency and national security confidentiality in both the open government and open court contexts. Given the subject matter of this paper – government secrecy – this is no easy task. It is difficult to arrive at definitive conclusions about whether government has properly balanced secrecy and disclosure, since an external researcher does not have access to the full range of information guarded on national security grounds by the government. Conclusions depend, therefore, on anecdote and partially tested hypothesis. With that caveat, in this section I nevertheless contend that Canada's record in maximizing open government and courts while protecting national security confidentiality is less than fully satisfactory. The Canadian approach suffers from both a failure of design and serious difficulties in implementation. Reform efforts, meanwhile, are burdened with their own shortcomings.

Difficulties of design

Open government

The already sufficient Access Act

Put simply, the national security limitations on open government are poorly planned and integrated. The most thoughtful law is the *Access Act*. The national security exceptions in this statute are fairly precisely defined,

creating intelligible standards and not simply invoking "national security" or "secret" or some other murky concept. In many instances, the Act includes an injury requirement, precluding disclosure only where there is some deleterious impact on a usually defined national security interest associated with the release of information. Moreover, almost all of the national security exemptions are discretionary, which implies that in making decisions on disclosure the government would have to balance the interests involved rather than impose a strict nondisclosure requirement.

The excessive Canada Evidence Act

Unfortunately, the relative clarity of the *Access Act* is not matched by the 2001 changes to the *Canada Evidence Act* (*CEA*). First, as the discussion above makes evident, the *CEA* creates three different classes of information: potentially injurious information, defined as "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security"; sensitive information, defined as "information relating to international relations or national defence or national security" that the government is safeguarding; and, in the context of attorney general's certificates, "information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security." The first concept – potentially injurious information – is generally consistent with the injury-based exemption in the *Access Act*. However, the other two concepts are significantly broader and very uncertain as to their precise scope. In no case are the terms "international relations," "national defence" or "national security" defined, leaving these concepts to be decided by the eye of the beholder.

Second, while the *Canada Evidence Act* provisions anticipate adjudication of government national security claims in court, and expressly enable the Federal Court to balance public interests in arriving at outcomes, this process may be short-circuited by the issuance of an attorney general's certificate. This certificate not only quashes any decision by a Federal Court judge to order the release of information under the *CEA*, but it also may be employed to quash proceedings under the *Access Act*. Subsequently, the government's judgment in issuing a certificate is subject to scrutiny only via a limited appeal to a single judge at the Federal Court of Appeal, who considers only if the government's reasons "relate to" national security or the other justifications listed in the Act (whatever that might mean).

The added government secrecy muscle that the *CEA* grafts onto the *Access Act* is particularly troubling, given the failure to carefully define the national security grounds justifying the issuance of a certificate. In other words, the careful attention to detail and balancing found in the *Access Act* is entirely circumvented by a *CEA* provision that provides minimal guidance on when governments are empowered to issue certificates.

The then information commissioner considered the 2001 amendments to be an unnecessary overreaction: "the *Access to Information Act* posed no risk of possible disclosure of sensitive intelligence information...no such information had ever been disclosed under the Act in the 18 years of its life and...the *Access to Information Act* régime offered as much or more secrecy to intelligence information as do the laws of our allies."[76] This conclusion is supported by Wesley Wark's assessment concerning the sufficiency of national security protection under the regular *Access Act* exemptions, noted above.

The unconstitutional antileakage provision

Lurking in the background, meanwhile, is the *SOIA*, and its unconstitutional section 4. Under section 4 of that act, unauthorized disclosure of even nonsecret but "official" government documents brings with it the possibility of criminal prosecutions. Where the document is "secret" within the (undefined) meaning of the Act, the prospect of being found criminally culpable increases and could include a situation where the document is shared internally within the government itself. Further, since the Act extends to "persons" and not just civil servants, and because it criminalizes receipt as much as disclosure, it makes leaked government information a "hot potato" that most risk-averse people would rather not receive. The net effect cannot be other than to chill the sharing of information, even when there may be a clear public interest in disclosure and dissemination.

The risks posed by the inarticulate section 4 are reduced by the *O'Neill* decision, but not eliminated. *O'Neill* is merely persuasive in other courts, it is not technically binding. Section 4 remains on the statute books, and it should not be expected that every official inclined to seek (or issue) a warrant under this provision, or threaten a prosecution, will be deterred by (or necessarily aware of) the constitutional critique of a single Ontario lower court, especially as time

passes. The recent DFAIT report on the Bernier-Couillard matter appears to be a striking case in point. As is now well known, then foreign affairs minister Maxime Bernier left classified briefing documents at the home of his partner at the time – Julie Couillard. Apparently, because Couillard delayed returning the documents, despite opportunities to do so, the DFAIT report declares that "Ms. Couillard may have put herself in potential jeopardy of having contravened a provision of the *Security of Information Act*" (Foreign Affairs and International Trade Canada 2008). The only conceivable provision of the *SOIA* at issue in the Bernier-Couillard affair is section 4.[77] An official government report has, therefore, intimated criminal liability – and likely precipitated reputational and other consequences – apparently based on a statutory provision declared unconstitutional by an Ontario trial court.

In sum, Canada is left with an antileakage provision whose doubtful reliability in a prosecution makes it an uncertain, counterproductive but still frightening tool. In an era when Canada is anxious about its international credentials in the security and intelligence community, it is worth noting that the *SOIA* compares unfavourably to its closest equivalent, the UK *Official Secrets Act* of 1989.[78] Certainly, in some respects, this UK law is less measured than its Canadian counterpart. Thus, the UK Act does include provisions that cover the security services and that are broadly equivalent to the Canadian statute's "persons permanently bound by secrecy" sections. Here, the UK Act is more unforgiving, imposing a blanket prohibition on unauthorized disclosure of "any information, document or other article relating to security or intelligence" in the person's possession by virtue of his or her employment in the security services.[79] There is no requirement that the damage stem from the disclosure. Further, unlike the Canadian law, in the UK law there is no public interest exception. The sole defence anticipated by the Act is if the person did not know of the security or intelligence nature of the information.[80]

Yet, insofar as its other leakage provisions are concerned, the UK Act is much more moderate (and intelligible) than section 4 of the *SOIA*. Thus, the UK Act makes it an offence, in section 1, for a civil servant to disclose information relating to security or intelligence, but only if this disclosure is damaging. This damage is measured by any actual damage it causes to "the work of, or of any part of, the security and intelligence services." Alternatively, that civil servant is liable if the information is of the sort that disclosure is "likely to cause such damage."[81] Ignorance of the security and intelligence nature of the information is a defence, as is the reasonable absence of belief that disclosure would be damaging.

Parallel provisions regulating disclosure of information relating to "defence" and to "international relations" are contained in sections 2 and 3 of the UK Act. The concepts of "defence" and "international relations" are both defined. Further, in both sections the disclosure is only an offence if it causes damage, a concept spelled out in detail in each instance. A lack of knowledge (or reasonable belief as to such knowledge) of the subject matter of the information is again a defence.

The UK Act also creates other offences for secondary leaking of secrets by recipients of wrongfully leaked documents. Thus, a person who receives a document relating to defence or international relations commits an offence under section 5 if he or she subsequently discloses it, knowing or having reasonable cause to believe that the information is protected by section 2 or 3. However, this subsequent disclosure must itself be damaging and the person must know, or have reasonable cause to believe, the disclosure to be damaging.

Thus, unlike the draconian section 4 of the *SOIA*, the UK Act carefully defines the sorts of information at issue in the criminalization of disclosure. Also unlike the Canadian law, it includes a requirement that disclosure of even this sensitive information be "damaging" (within the meaning of the Act) before there is criminal culpability.

Open courts

Canada's open government laws are not alone in being internally incoherent. A similar lack of consistency plagues Canada's rules on disclosure in court proceedings. As noted, section 38 of the *CEA*'s definitions of information that can be guarded on national security grounds are ambiguous. However, that Act at least establishes a balancing regime, in which national security interests can be weighed against, *inter alia*, the public interest in fair trials. That balancing is potentially truncated by the nuclear bomb of an attorney general's certificate (to date, never used), but a trial court in criminal matters retains the discretion to toss the government's case if the government refuses to disclose enough information to preserve a fair trial.

In comparison, the information disclosure regime established by the security certificate system under the *IRPA* has no such nuance. Information is withheld if necessary on national security grounds (without

any effort to define this concept). There is no balancing, and there is no possibility that a court can dismiss the proceeding because the level of disclosure has been inadequate.

For the latter reason, the security certificate system is out of line not just with the approach adopted by the *CEA*, but also with that evolving in the United Kingdom in the wake of the House of Lords' recent decision of *Secretary of State v. MB*.[82] In that decision, the House of Lords examined the compatibility of the UK system of "control orders" – limitations on liberty imposed on the basis that a person is suspected of posing a terrorist threat – with the European Convention on Human Rights. Control orders proceedings include the use of secret evidence. In reasoning that will almost certainly affect UK national-security-related immigration proceedings as well, the law lords suggested that a residual discretion rests with the judge to determine whether the level of disclosure to the interested person suffices to meet fair trial standards. Where the proceeding falls short of a fair hearing, the matter might come to an end, unless the government is prepared to make fuller disclosure.[83]

Difficulties in execution

These shortcomings in design are augmented by acute problems in execution. Even with a thorough redrafting of Canada's secrecy laws, with ample attention to definition and precision, problems of execution would almost certainly continue to plague efforts to reconcile transparency with security. Indeed, problems exist in the Canadian system, even though one of the most critical structural shortcomings identified above – the attorney general's certificate under the *CEA* – has not been used to date.

The eye of the beholder

The single largest challenge in execution is probably the problem of subjectivity. Information in the possession of government is, in the first (and often final) instance, assessed for disclosure by government officials themselves. Even acting in the utmost good faith, individual officials will vary in their assessments of whether a given document contains, for instance, information that could reasonably be expected to be injurious to the defence of Canada or an allied state. This variability almost certainly increases as definitions of information to be withheld become more ambiguous; that is, simply invoking "national security." Individual subjectivity may be compounded by differing "cultures" of secrecy versus transparency that evolve in different government departments in different eras. Discussing this problem in the American context as it existed in the Cold War, then senator Daniel Patrick Moynihan noted that "To preserve an open society it was deemed necessary to take measures that in significant ways closed it down" (United States, Commission on Protecting and Reducing Government Secrecy 1997). In a "culture of secrecy," the propensity is to overclassify, and power is sometimes derived from withholding secrets and revealing them only to a select few.

Establishing the effects of this postulated subjectivity (and culture) is difficult. Anecdotal evidence tends, however, to point to its existence and importance. For example, critics have repeatedly complained of the Department of National Defence's ready reliance on national security exceptions under the *Access Act*. In some instances, exemptions have been applied to information that is already publicly available. According to media reports from 2006, "In an examination of 23 access requests made to the Defence Department over the last 18 months, 87 pieces of information, now censored, had been previously released to the public or are still on government and Defence Department websites" (Pugliese 2006). This observation adds empirical substance to a chorus of opinion accusing the current government of excessive secrecy, especially in relation to Afghanistan.[84] It also shows how mores and views on the need to censor particular bits of information vary over time.

The "mosaic effect" and overclaiming

As a related issue, there is serious reason to believe that national security confidentiality produces "overclaiming" – that is, a propensity to assert secrecy where it is not truly warranted. Again, proving a systematic propensity to overclaim is next to impossible. Overclaiming has, however, been an acute issue in a number of recent cases. Most famously, in his factual report in the Arar inquiry, Justice O'Connor commented on the government's propensity to overclaim as follows:

> the public hearing part of the Inquiry could have been more comprehensive...if the Government had not, for over a year, asserted NSC [national security confidentiality] claims over a good deal of information that eventually was made public, either as a result of the Government's decision to re redact certain documents beginning in June 2005, or through this report...This "overclaiming" occurred despite the government's assurance at the outset of the inquiry that its

> initial NSC claims would reflect its "considered" position and would be directed at maximizing public disclosure. The Government's initial NSC claims were not supposed to be an opening bargaining position...It is perhaps understandable that, initially, officials chose to err on the side of caution in making NSC claims. However, in time, the implications of that overclaiming for the Inquiry became clear. I raise this issue to highlight the fact that overclaiming exacerbates the transparency and procedural fairness problems that inevitably accompany any proceeding that can not be fully open because of NSC concerns. It also promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality. It is very important that, at the outset of proceedings of this kind, every possible effort be made to avoid overclaiming. (Commission of Inquiry 2006, 301-2)

The Arar inquiry is not, of course, the only one probing government national security secrets. Others include the 2006 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Air India inquiry),[85] and the 2006 Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Iacobucci Commission).[86]

Anecdotally, I have the impression that the various judicial inquiries on national security matters have exposed overclaiming, pressed the government logic for secrecy in many instances and perhaps produced a slightly more critical internal assessment by government of secrecy justifications. It is impossible to measure how meaningful this adjustment has been, or whether it will have lasting impact. Nor is it clear that a key countervail to this slight opening – the deep secrecy generated by Canada's military operations in Afghanistan – will sweep away whatever gains were made through the era of inquiries.

At any rate, it is true that whatever impact pressure mounted on the government through the inquiry process had on government secrecy doctrine, government overclaiming persisted even in relation to the final report in the Arar matter. In a *CEA* proceeding, the Federal Court ultimately ordered disclosure of a handful of additional lines that the government wished censored from the report. In the course of his reasoning, Justice Noël noted that the "Court will not prohibit disclosure where the Government's sole or primordial purpose for seeking the prohibition is to shield itself from criticism or embarrassment."[87] The court did not connect this statement to the information ultimately released. That information was, however, embarrassing to the government, demonstrating (among other things) that the government was aware of the American policy of "rendition" and the likelihood that Arar was being removed to Syria to be tortured. Commenting on the Arar experience, Kent Roach has observed:

> The subsequent release of the majority of the disputed passages in the Arar Commission's report affirmed for many that the government had overclaimed NSC and used it to shield information that was embarrassing to the government and its allies but that did not protect the lives of informers or ongoing operations. Such findings affect the government's credibility. There is a danger that the wolf of national security confidentiality will be called too often. (2008)

Indeed, the Arar case is apparently not exceptional. In several more recent *CEA* cases, the Federal Court has disagreed with the government's secrecy claims and ordered information released. In *Khawaja,* for example, Justice Mosley offered the following observation about the government's propensity to excise every reference to CSIS from material at issue in that criminal proceeding:

> CSIS has acknowledged an investigative interest in the respondent up to his arrest on March 29, 2004, assistance and involvement with surveillance of his movements and their presence on the date of the RCMP search of his home. But those holding the black pens seem to have assumed that each reference to CSIS must be redacted from the documents even where there is no apparent risk of disclosure of sensitive information such as operational methods or investigative techniques or the identity of their employees. I acknowledge that there can be instances in which an informed reader will connect the dots to obtain such information but that does not apply in every case.[88]

It may be that overclaiming is almost an inevitable outcome of national security confidentiality – no government official wishes to be the one to disclose information that ultimately proves prejudicial. The natural propensity may be, therefore, to err on the side of secrecy. However, it seems likely that this understandable human instinct is compounded by official doctrines that encourage overclaiming. Justice Mosley's reference to connected dots is no passing reference. Chief among government secrecy doctrines is the so-called "mosaic effect," a concept that has been invoked frequently by the Canadian government.[89]

Put simply, the mosaic effect posits that the release of even innocuous information can jeopardize national security if that information can be pieced together with other data by a knowledgeable reader. The result is a mosaic of little pieces of benign information that cumulatively discloses matters of true national security

significance. As urged by one CSIS official in a public affidavit in the Federal Court:

> assessing the damage caused by disclosure of information cannot be done in the abstract or in isolation. It must be assumed that information will reach persons with a knowledge of Service targets and the activities subject to this investigation. In the hands of an informed reader, seemingly unrelated pieces of information, which may not in themselves be particularly sensitive, can be used to develop a more comprehensive picture when compared with information already known by the recipient or available from another source.[90]

The mosaic effect has been accepted by Canadian courts, and it has guided decisions on disclosure. As noted by the Federal Court in one of the first cases to apply the doctrine,

> in security matters, there is a requirement to not only protect the identity of human sources of information but to recognize that the following types of information might require to be protected:...information pertaining to the identity of targets of the surveillance whether they be individuals or groups, the technical means and sources of surveillance, the methods of operation of the service, the identity of certain members of the service itself, the telecommunications and cypher systems and, at times, the very fact that a surveillance is being or is not being carried out. This means for instance that evidence, which of itself might not be of any particular use in actually identifying the threat, might nevertheless require to be protected if the mere divulging of the fact that CSIS is in possession of it would alert the targeted organization to the fact that it is in fact subject to electronic surveillance or to a wiretap or to a leak from some human source within the organization.[91]

There is an obvious logic in this reasoning, especially if one is confronted with a well-resourced and sophisticated adversary with the means to pull together inchoate pieces of information into a prejudicial whole. However, the use of the mosaic effect outside the context of security investigations involving confidential informers and techniques could greatly erode open government and open courts. Since the doctrine applies to innocuous information, the future use of which can never be predicted, it could be deployed to stave off disclosure of virtually *any* piece of information. Further, the mosaic effect is a creature of the Cold War, when the chief adversaries were Eastern Bloc intelligence services. Its uncritical application to cases involving, for example, much more diffuse and indefinite terrorist threats may not be warranted.[92]

There must therefore be an outer limit where even information related to an investigation is disclosable. Some information is so innocuous that it strains plausibility to maintain that it must be kept secret. In *O'Neill v. Canada*, for example, the RCMP resisted disclosure on national security grounds of the location of an RCMP building, "even though it has an exterior sign indicating that it is an RCMP building."[93] Moreover, the location of the building had already been disclosed in the Arar inquiry. Not surprisingly, the Ontario Superior Court of Justice ordered the release of the information in the *O'Neill* proceedings.

The Federal Court also appears attuned to the difficulties in applying the mosaic effect theory and has now expressed frank skepticism of the doctrine: "Witnesses from the intelligence community may take the mosaic effect theory as an article of faith, relying upon it as a complete answer to the release of information they consider sensitive or potentially harmful. As stated by Justice Noël in *Arar*...'Simply alleging the effect is not enough. There must be some basis or reality for such a claim based on the particulars of a given file.'"[94] Thus, "by itself the mosaic effect will usually not provide sufficient reason to prevent the disclosure of what would otherwise appear to be an innocuous piece of information. Something further must be asserted as to why that particular piece of information should not be disclosed."[95]

The "third party" trump card

As noted above, secrets shared by allied governments are given robust protection in Canadian information law. However, blanket prohibitions on disclosure because of simple foreign provenance give secrecy law an extended reach in an intelligence-importing country like Canada. It is not likely that every piece of foreign information must be held secret because it would jeopardize the security interests of the providing state. Guarding information simply because of foreign origin inevitably "launders" innocuous information and restricts the universe of disclosable information.

Recently, a number of court decisions have raised questions about the reach of the third party rule. In *Khadr*, Justice Mosley commented as follows: "it is my view that too much of the routine communications between foreign and Canadian agencies is protected by the Attorney General in application of the third party principle. In this case there were examples that simply did not stand up to scrutiny."[96]

Accordingly, in this and other cases, the courts have tempered the circumstances in which the third

party rule will be accepted. At the very least, the government should be obliged to seek permission to disclose from the foreign source in an effort to separate truly sensitive information from more benign data. This is an obligation that probably already exists in the *Access Act* and *Privacy Act* contexts[97] and has also been invoked by the Federal Court in relation to the *CEA*.[98] In the latter context, the court examines whether "good faith efforts were made and continue to be made to obtain such consent."[99]

Moreover, the government cannot claim "third-party" confidentiality over information that it has obtained from a foreign partner, but it has received also by other means. Refusal to disclose this information must instead be grounded in another justification.[100] Nor can third party confidentiality be used "to protect the mere existence of a relationship between Canada and a foreign state or agency, absent the exchange of information in a given case."[101]

Overwhelmed checks and balances

As this discussion suggests, many of the shortcomings in Canadian law and policy could be overcome by robust checks and balances that query subjectivity and overclaiming in national security confidentiality. The Federal Court has been particularly active in the past three years in developing more demanding standards for government secrecy in the national security area.

The Federal Court's influence in this area is, however, limited to judicial proceedings, such as those under the *CEA*. While in principle disputes over transparency under the *Access Act* could end up in front of the court, they do so infrequently, and usually only when backed by requesters with unusually deep pockets. Most denied requests or redacted disclosures go unchallenged or, at best, are funnelled into the information commissioner's complaints process. The commissioner's scrutiny of government decisions can be meaningful. As described by the Commons access to information committee,

> where the Commissioner investigates a discretionary exemption, such as section 15(1) of the ATIA [*Access Act*], his office will require the head of the government institution to explain the factors, pro and con disclosure, that were weighed in exercising the discretion. The Commissioner will then assess whether these were the correct factors to be taken into consideration and whether they were given the appropriate weight. Where the exemption is injury-based, the Commissioner will also look to ensure that there is a reasonable basis for an expectation of injury should the information be disclosed. (House of Commons Standing Committee on Access to Information, Privacy and Ethics 2008)

Unfortunately, the *Access Act* complaint process is mired in significant delays – in 2007-08, the information commissioner's office closed complaints in eight months, on average (Information Commissioner of Canada 2008), a period almost double that at the beginning of the decade (Information Commissioner of Canada 2000). These delays are in addition to the now regular delays by the government in processing the initial request. In 2007-08, the responses to over 40 percent of access requests took longer than the statutory default of 30 days – and a sizeable minority (13 percent) took longer than six months (Treasury Board of Canada Secretariat 2008).

In sum, the vast bulk of government balancing of transparency versus national security confidentiality is either unexamined by arm's length observers, or examined only after prolonged delay.

Reform minimalism

The challenge of addressing problems in reconciling transparency with national security confidentiality is made more difficult by the Canadian approach to reform. There is little evidence that the government or legislators have much interest in revising, refining and improving Canada's information laws. We are burdened, it would seem, with inconsistent and (in the case of section 4 of the *SOIA*), incoherent and ineffectual laws. Moreover, where changes are made, they tend to be minimalist; that is, the government selects (and Parliament endorses) approaches that maximize secrecy at the expense of transparency. A case in point is the new "special advocate" system introduced into the security certificate system in the wake of the Supreme Court's 2007 *Charkaoui* decision.

The Supreme Court released the *Charkaoui* decision on February 23, 2007, finding the immigration security certificate system (as it then existed) unconstitutional. Specifically, the Court held that the system's secrecy rules violated section 7 of the Charter. This secrecy was not saved by section 1; the government had shown no reason why it had failed to adopt some sort of model in which an independent "special counsel" represented the interests of the named person in the secret portions of the proceedings.

Critically, in the course of its decision, the Court canvassed a number of different special counsel options, but without expressing a preference between these alternatives. Indeed, it expressly left it to Parliament to decide "what more should be done."[102] These alterna-

tives were (in the order in which they appeared): the SIRC process; the Air India trial process; the Arar Commission process; and the United Kingdom system of special advocates. It also discussed the approach taken by the *CEA* in the disclosure of information said to raise national security issues.

The Court suspended its declaration of constitutional invalidity for one year, until February 23, 2008, in order to allow a reaction from Parliament. Not surprisingly, in the immediate aftermath of the *Charkaoui* decision, the policy focus was on "special counsel." For instance, a month after *Charkaoui*, a special Senate committee recommended that a special counsel process be extended to all proceedings where "information is withheld from a party in the interest of national security and he or she is therefore not in a position to make full answer and defence," including under the *IRPA*, the Criminal Code terrorist group listing process, the *Charities Registration (Security Information) Act*[103] and the *CEA* (Special Senate Committee on the *Anti-terrorism Act* 2007, 42). Moreover, the committee urged that the special counsel be empowered to communicate with the affected parties after receiving confidential information, subject to guidelines designed to bar the release of secret information. The counterpart Commons committee also recommended a comprehensive "panel of special counsel" for national security cases (House of Commons Standing Committee on Public Safety and National Security 2007, 81), but without weighing in on the precise design of this system.

The government, for its part, remained largely silent. Despite the notoriety of the security certificate system and the controversy sparked by it, no public consultations were held and no formal notice was given of the government's approach to the special counsel issue until Bill C-3 was tabled in the House of Commons and received first reading, on October 22, 2007 – fully eight months after the *Charakoui* decision and four months prior to the expiry of the one-year suspension of the declaration of invalidity.

As noted above, the Supreme Court of Canada canvassed a number of special counsel options in *Charkaoui* without mandating a particular model. The government was therefore presented with a choice in the crafting of Bill C-3, which included building on Canada's indigenous experience with SIRC in immigration and other matters. This SIRC approach was employed in security certificates against permanent residents up until 2002, and it is still applied in relation to SIRC's investigation of complaints against CSIS. In the SIRC model, SIRC counsel (whether in-house or outside legal agents retained by SIRC) are permitted to communicate throughout the process with the interested party and his or her counsel. They are obliged, of course, not to reveal secret information but may continue to pose questions of a sort that does not betray such a secret in order to better understand the facts. No SIRC in-house or outside counsel has ever reportedly received any complaints from the government that this contact with the named person has resulted in an involuntary disclosure injurious to national security (see Forcese and Waldman 2007). As Gordon Cameron, an experienced SIRC legal agent, has noted: "To my knowledge, these interviews have been conducted without any inadvertent disclosure of information and I am not aware that CSIS has ever complained about or attempted to change this practice."[104]

At the same time, this continued contact has been elemental in preserving a fair process. In Cameron's words:

> In my work in SIRC hearings, there have been a number of occasions on which the ability to question the complainant after reviewing the confidential information has allowed SIRC in-house counsel and me to advance the interests of complainants on both of the afore-mentioned bases; that is, to disprove or cast incriminating allegations into doubt, and to rebut or qualify allegations of deceitfulness.[105]

In comparison, the UK-style "special advocate" model imposes extremely strict restrictions on continued contact between the special advocate and the named person once the former has reviewed the secret information. In effect, there is no communication at all. The Supreme Court itself was alive to criticisms of the UK system, including those concerning restrictions on contact between the named person and the special advocate.[106] Nevertheless, for reasons that have never been satisfactorily explained to this author, the government opted for the secrecy-maximizing and fair-trial-minimizing United Kingdom approach.[107]

As Kent Roach observes, in so doing the government selected, and Parliament ratified, "the only alternative that the [Supreme] Court recognized [in *Charkaoui*] had been subject to criticism and the one alternative that arguably achieves the worst job of all the alternatives in ensuring fair treatment of the affected person" (Roach, forthcoming). Parliamentarians themselves were clearly aware of this problem. When the Bill was debated in the Senate, even a Conservative Senator expressed concern: "Sometimes we hold our noses when it comes time to adopt bills, and we have done so in the past with other legislation, knowing that in the near future we will correct the errors we have agreed to let through. That is the sort of legislation we have before us now."[108]

Conclusion and Recommendations

In sum, Canada's information and secrecy laws and practices leave much to be desired. Past commentary from the security and intelligence community itself suggests that the breadth of secrecy laws is more than is necessary to protect legitimate national security secrets. At the same time, the incoherence of these laws, the uncertainty this incoherence produces and the overclaiming it allows create conditions likely to curb benign information exchanges, at great expense to the credibility of the security services. Finally, the limits they impose on information access – and the draconian penalties they level in some instances – are deeply inconsistent with the democratic society they are supposed to protect. They are broad enough to let government sidestep embarrassment and mask incompetence, all in the name of national security.

In these concluding sections I propose several "quick fixes" for this problem. It is worth acknowledging, however, that fixes are easy to imagine and difficult to implement, in a significant measure because of the difficult policy environment in which national security issues are addressed. Not least, national security law responds to uncertain dangers, while at the same time straddling conventional subject-matter divisions in the policy and parliamentary communities. The Commons, for example, has a (relatively new) national security committee, but it also has separate committees dedicated to justice, immigration, and privacy and access to information.

At the bureaucratic level, the development of different statutes grappling with different national-security-related issues is centred in different departments. Meanwhile, operating independently of these departments are the auditor general and the privacy and information commissioners, specialized officers of Parliament, whose mandates extend to several areas of law affected by antiterrorism statutes. There is, however, no officer of Parliament whose writ reaches across all of national security or even antiterrorism law. Within the security and intelligence community itself, arm's length review responsibilities are "stovepiped" between the Security Intelligence Review Committee (for CSIS) and the commissioner of Communications Security Establishment Canada (for CSE). No equivalent body existed at the time of this writing for the RCMP.

Meanwhile, within the academic community, only a handful of scholars specialize in national security or antiterrorism law per se, and courses in antiterrorism or national security law are taught in only a handful of law schools. Instead, academics tend to have more specialized expertise in criminal, privacy or immigration law, for example.

All of these actors are asked to grapple, in a democratic policy-making environment, with a threat that is often inchoate in nature. As Lynch notes, "it is extremely difficult for parliamentarians to know the true extent of the threat to the nation's security when trying to insist either upon a more consultative, careful process or the inclusion of specific powers and safeguards" (2006). For all of these reasons, national security law is an area in which trees may sometimes attract scrutiny more readily than does the forest; that is, attention is drawn to a handful of particularly controversial areas, leaving the vast bulk of national security measures unexamined in any detail. National security confidentiality is unquestionably one of these orphans – the *Security of Information Act*, for example, has attracted relatively little attention from parliamentarians, even with the sweeping renovations made to it in 2001 as part of the massive *Anti-terrorism Act*, and even after the *O'Neill* decision.[109]

Nevertheless, despite these difficulties, I envisage four fixes that would go a long way in rebalancing the secrecy law regime and undergirding the culture of openness required in a functioning democracy.

Correcting the *Security of Information Act*

First, Parliament should formally repeal section 4 of the *Security of Information Act* (*SOIA*), replacing it with a much more measured provision. Despite the condemnation of the Ontario Superior Court of Justice, section 4 sits lurking on the statute book as a big stick to be deployed by inattentive officials. The recent provisions relating to persons bound by secrecy penalize leakage from the intelligence services. With the repeal of section 4, a more measured provision covering other civil servants and persons receiving protected information would have to be drafted. In this respect, the new law could follow the precedent of the UK *Official Secrets Act* by defining extremely carefully and narrowly the sorts of secrets covered by criminal provisions, and by introducing a prerequisite that damage, as defined by the Act, stem from disclosure. The amended *SOIA* could then apply a public interest override of the sort currently available to persons bound by secrecy.

Coherent redrafting and integration of information law

Second, the government should standardize its definition of "national security" (and similar terms, such as

"national defence" and "international relations") across the statute book. Currently, exemptions from disclosure on national security grounds are conveyed by a confusing array of terms, such as "international affairs, national defence and national security," "national security," "security of Canada," "Canadian interests," "information that is of a type that the Government of Canada is taking measures to safeguard."

It makes sense, as a first step, to harmonize what the government means by national security. To a certain extent, the government has already done this with the term "security of Canada" in the *CSIS Act*. Employing this definition in lieu of other, undefined references to "national security" or its similes in the Canadian statute book would have two salutary effects. First, it would provide a necessary metre stick against which to measure the legitimacy of national security justifications in the many statutes that lack a definition of the term. Second, it would standardize and centralize the understanding of national security throughout Canadian federal law. Debate could then focus on the adequacy of this standardized and centralized definition and not be distracted by questions of whether national security might be approached differently in the other, sometimes obscure circumstances in which statutes invoke it.

It is true, however, that the concept of the "security of Canada" defining the mandate of CSIS may not always overlap with the classes of information that the government seeks legitimately to protect on national security grounds. Special definitions of national security secrets will also have to be articulated. For instance, the *SOIA* has attempted to provide a definition of national security secrets with its concept of "special operational information." The *Access Act*, meanwhile, has comprehensive definitions for its national security exemptions. Lining up these two sources of definitions of national security secrets and then using this reconciliation to contribute greater certainty to the invocation of international relations, defence and national security in the *CEA* and other statutes, such as the *IRPA*, will require some modest redrafting.

In this respect, section 15 of the *Access Act* is the logical nexus point for a common understanding of national security secrets. First, its use of the expression "international affairs" should be defined. A starting point might be the UK *Official Secrets Act* of 1989, which defines international relations as "any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation."[110] Second, the reference to "prevention or suppression of subversive or hostile activities" in subsection 15(1) should be replaced with "national security." The section should then define "national security" according to the proposed, standard definition in the *CSIS Act*. Finally, section 15 should also capture "special operational information," as defined by the *SOIA*.

The *CEA* should be amended to eliminate its creation of three new and slightly different classes of national security information. Instead, the Act should only apply to "potentially injurious information," defined to mean information specified in section 15 of the newly amended *Access Act*. A similar change should be made to the *IRPA*'s security certificate rules.

Notably, fixing section 15 as the litmus test would incorporate that section's injury test into the *CEA* and *IRPA*. Such a change would probably add little to regular *CEA* section 38 determinations. This section already incorporates an injury test and allows a Federal Court judge to contemplate the balance of public interests in reaching a disclosure decision. The proposed amendment would, however, provide greater latitude for a Federal Court of Appeal judge to contemplate the balance of interests in assessing the merits of an attorney general's certificate issued under the Act. Likewise, judges in the *IRPA* context could also complete a balancing.

In essence, the amended *CEA* would allow the minister to certify *Access Act* section 15 information as exempt from the *Access Act*, disallow its use in proceedings, and bring it under the different appeal and review regime established by the *CEA*. These are still extremely potent powers. In the absence of compelling evidence that more is needed, these changes seem more than sufficient to secure legitimate government secrecy.

These amendments would not put national security at risk. Disclosure would still be carefully circumscribed by the now even more generous *Access Act* exemptions – exemptions that the Canadian security services saw as sufficient even before the new post-9/11 restrictions. On the other hand, these changes would simplify and standardize government secrecy law, eliminate much uncertainty as to its scope and leave good governance in Canada less dependent on benign executive branch interpretations of today's perplexing secrecy laws.

Institutional reforms

Third, the government should address the institutional failings of the access regime. Better resourcing of the information commissioner's office to permit the expeditious review of complaints is a pressing need.

That office should be particularly attentive to overclaiming in the national security area, taking its lead from the more critical eye being cast on government secrecy claims by the Federal Court.

Enhancing the information commissioner's capacity is not, however, enough. Part of the burden on that office would be reduced if the government's application of the *Access Act* was more credible in the first instance. In this regard, better resourcing and training of the front-line access personnel who manage information requests received by their departments is desirable. The anecdotal evidence cited above suggests that consistent and standardized application of national security exemptions remains a challenge. Sincere recognition that timely responses to information requests are part of a public official's obligations – and the resources to back that recognition up – might also resolve some of the *Access Act*'s challenges.

Attentiveness to overclaiming should also figure among the responsibilities of the various specialized national security review bodies – such as the SIRC, the CSE commissioner and other security services (should the Arar Commission's policy recommendations ever be implemented). Annual reviews of agency performance by these bodies should include close attention to agency information disclosure philosophies and practices.

Lastly, the security intelligence services themselves (and central government agencies such as the Privy Council) should carefully consider whether, on balance, information can reasonably be withheld. As then US representative Lee Hamilton observed in 1997, "If we have too much secrecy, we cannot focus enough on protecting the truly important secrets. Secrecy can best be preserved when the credibility of the system is assured" (Hamilton 1997). Overclaiming does no service to those instances where bona fide national security preoccupations require secrecy. The risk, when overclaiming is revealed, is that claims to secrecy thereafter are viewed as cries of wolf by the public, the media and (potentially) the courts. To its credit, there is some evidence that the security and intelligence community understands this, and I and a number of academics have recently been party to unusually frank discussions with at least one agency that have served to enlighten without imperilling national security.

At core, changing government attitudes are ultimately at the heart of a renewed culture of openness. Indeed, such a sea change seems now to be underway in the United States, with the Obama administration's firm pronouncement on the need to adhere fully to the US *Freedom of Information Act* and to apply a presumption of disclosure (Presidential Documents 2009).

Sustained parliamentary attention

Last, Parliament itself should demonstrate a healthy skepticism of government secrecy claims on national security grounds. The Standing Senate Committee on National Security and Defence did so in its 2003 report on airport security. Legislators were, however, willing to pass amendments to the security certificate process that overreach in the defence of secrecy at the expense of fairness in the judicial process.

Given the later experience, I may be accused of being irremediably naive to expect much of parliamentarians in the areas at issue in this paper. On the other hand, contempt of Parliament and its ability to show measured contemplation on national security questions will produce nothing but a vicious circle in which a distracted and disinterested Parliament, treated as inept in this area, is given short shrift and is stripped of any opportunity to gain experience, insight and authority. In other works, I have expressed support both for a standing reviewer of national security law and policy and a separate committee of parliamentarians, with legislated powers and access to secret information (and subject, concomitantly to nondisclosure obligations) (Forcese 2008). I renew that call as a conclusion to this paper.

Last words

Individually or collectively, there is no reason to believe that any of the changes I have proposed would produce the feared "sinking ships" said to be produced by "loose lips." Legitimate secrets would be protected. At the same time, these reforms might remove government secrecy laws as an obstacle to legitimate public scrutiny, and in so doing actually enhance security. To paraphrase the Standing Senate Committee on National Security and Defence, public pressure could do exactly what secrecy might fail to do: motivate governments to repair the holes that do sink ships.

Notes

1 The phrase was an allusion to the dangers to Atlantic convoys of German foreknowledge of sailing times and routes.

2 Similar comments have been made by academic observers. "Freedom of expression and access to information, by enabling public scrutiny of government action, serve as safeguards against government abuse and thereby from a crucial component of genuine national security" (Coliver 1999, 11-12); "The problem with the 'national security state' is not so much that it violates [fundamental] rights, although it sometimes does just that, but that it can lead to the repetition of irrational decisions" (Chevigny 1991, 138).

3 *Freedom of Information Act* of 4 July 1966, Pub. L. No. 89-487, 80 Stat. 250 (5 U.S.C. § 552).

4 Freedom of Information: Hearings on S. 1666 and S. 1663 before the Subcomm. on Admin. Practice and Procedure of the Senate Comm. on the Judiciary, 88th Cong. 3 (1964) (statement of Sen. Edward Long), cited in Wichmann (1998, 1217).

5 *NLRB v. Robbins Tire and Rubber Company*, 437 U.S. 214 at 242 (1978), 57 L Ed 2d 159 at 178.

6 Pierre Elliott Trudeau, quoted by G. Baldwin, MP, in *Minutes of Proceedings and Evidence of the Standing Joint Committee on Regulations and other Statutory Instruments*, 30th Parl., 1st Sess. (1974-75) 22:7, cited in Rankin (1979, 1).

7 *House of Commons Debates* (29 Nov. 1979) at 1858, cited in House of Commons Standing Committee on Justice and the Solicitor General on the Review of the *Access to Information Act* and the *Privacy Act* (1987, 4).

8 [1997] 2 S.C.R. 403 at para. 61, 148 D.L.R. (4th) 385.

9 For example, see *Canada (Attorney General) v. Canada (Information Commissioner)*, [2004] F.C. 431 at para. 22 (F.C.T.D.); *Yeager v. Canada (Correctional Service)*, [2003] 3 F.C. 107 at para. 39, 2003 F.C.A. 30; *Rubin v. Canada (Minister of Transport)*, [1998] 2 F.C. 430 at para. 36, 154 D.L.R. (4th) 414 (F.C.A.).

10 *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66 at para. 32.

11 R.S.C., 1985, c. A-1.

12 *AstraZeneca Canada Inc. v. Canada (Health)*, 2005 F.C. 1451 at para. 49 (F.C.), *aff'd*, 2006 F.C.A. 241.

13 *Canada Post Corporation v. Canada (Minister of Public Works)*, [1995] 2 F.C. 110 at 129, F.C.J. No. 241 (F.C.A.) ("subsection 4(1) contains a 'notwithstanding clause' which gives the Act an overriding status with respect to any other Act of Parliament").

14 *Access Act*, s. 30.

15 *Access Act*, ss. 41 and 42.

16 For example, see International Covenant on Civil and Political Rights (ICCPR), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976, Art. 14 (applicable to criminal proceedings and any suit at law determining rights or obligations, and requiring a "public hearing," except in limited circumstances such as when required by national security).

17 For example, see *Attorney General of Nova Scotia v. MacIntyre*, [1982] 1 S.C.R. 175, at 187; *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480 at paras. 21 & 22; *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 S.C.R. 1326.

18 Being Schedule B to the *Canada Act 1982* (U.K.) 1982, c. 11.

19 *Ruby v. Canada*, 2002 S.C.C. 75 at para. 52.

20 Ibid. at para. 53, citing *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480, at para. 23.

21 ICCPR, Art. 14(3)(b) specifies that an accused in criminal cases is "[t]o have adequate time and facilities for the preparation of his defence." The UN Human Rights Committee interprets "facilities" as including "access to documents and other evidence which the accused requires to prepare his case." UN Human Rights Committee, *General Comment 13*, U.N. Doc. HRI/GEN/1/Rev.6 at 135 (2003) at para. 9.

22 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326 at para. 17.

23 *R. v. Chaplin*, [1995] 1 S.C.R. 727 at para. 21.

24 *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 S.C.C. 38 at para. 43.

25 See, for example, Douglas Bland, appearing at the Standing Senate Committee on National Security and Defence, *Evidence* (October 29, 2001) (indicating that "if a broad definition of 'national security' is taken, there is a danger that there will be no obvious limits to policy," but then citing with a measure of approval the National Defence College definition).

26 CSIS affiant's testimony, reported in *Khawaja v. Canada*, 2007 F.C. 463 at para. 132.

27 Affidavit of Margaret Ann Purdy (then director general of the Counter-terrorism Branch) (31 Oct. 1994), cited in *Ruby v. Canada*, [1996] 3 F.C. 134 at para. 25 (F.C.T.D.).

28 Ibid. (court summary of affidavit).

29 Ibid. at para. 26.

30 Ibid. at para. 27.

31 See, for example, *Ribic v. Canada*, 2003 F.C.T. 10 at para. 10 (F.C.); *Khawaja v. Canada*, 2007 F.C. 490 (F.C.) at para. 122 *et seq.*

32 Ibid. at para. 127.

33 Jack Hooper, Assistant Director of Operations, CSIS, Testimony, Arar Commission, June 22, 2005, at 485.

34 Declaration of the Secretary of Defense, *United States of America v. Jonathan Jay Pollard*, United States District Court for the District of Columbia, Criminal No. 86 at 22, cited in Richelson (1999, 291).

35 These limitations are echoed in the *Privacy Act*'s provisions on disclosure to applicants of applicants' own personal information in the possession of government. See *Privacy Act*, R.S., 1985, c. P-21, ss. 12 *et seq.* Because the *Privacy Act*'s disclosure functions are limited to an individual's own personal information, the focus in this paper is on the *Access Act*.

36 See, for example, *Rubin v. Canada (Minister of Transport)*, [1998] 2 F.C. 430 at para. 36, 154 D.L.R.

(4th) 414 at para. 30 (F.C.A), citing *Canada Packers Inc. v. Canada (Minister of Agriculture)*, [1989] 1 F.C. 47 at 60 (F.C.A.) ("Subsection 2(1) provides a clear statement that the Act should be interpreted in the light of the principle that government information should be available to the public and that exceptions to the public's right of access should be 'limited and specific.' With such a mandate, I believe one must interpret the exceptions to access in paragraphs [20(1)] (c) and (d) to require a *reasonable expectation of probable harm*") (emphasis added).

37 R.S.C. 1985, c. C-23. See also *Privacy Act*, s. 22.

38 *Ruby*, 2002 S.C.C. 75 at para. 5.

39 *Access Act*, s. 15. See also *Privacy Act*, s. 21.

40 *Access Act*, subs. 15(2).

41 Ibid. The expression means: "espionage against Canada or any state allied or associated with Canada...sabotage...activities directed toward the commission of terrorist acts, including hijacking, in or against Canada or foreign states...activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means...activities directed toward gathering information used for intelligence purposes that relates to Canada or any state allied or associated with Canada, and...activities directed toward threatening the safety of Canadians, employees of the Government of Canada or property of the Government of Canada outside Canada."

42 S.C. 2001, c. 41.

43 R.S.C., 1985, c. C-5 (*CEA*).

44 *CEA*, s. 38. A "proceeding...means a proceeding before a court, person or body with jurisdiction to compel the production of information."

45 *CEA*, s. 38.13.

46 *CEA*, s. 38.131.

47 *Access Act*, s. 69.1.

48 2004 S.C.C. 43 at para. 4.

49 See, for example, s. 486 of the Criminal Code, R.S., 1985, c. C-46, the central provision in the Criminal Code curtailing the open court principle for criminal proceedings on national security grounds, as interpreted by the Supreme Court in *Vancouver Sun*, at para. 71. See also *Toronto Star Newspapers v. Canada*, 2007 F.C. 128 (F.C.), reading down those provisions obliging the Federal Court to hold a *Canada Evidence Act* application and records confidential and to hold the hearing in private to only those circumstances where the government requests an *ex parte* hearing.

50 *CEA*, s. 38.

51 *CEA*, s. 38.

52 For example, see Rosenthal (2003, 191) for a critique of this language.

53 *Khawaja*, 2007 F.C. 490 at paras. 62 *et seq.*; *Canada (Attorney General) v. Commission of Inquiry into the Action of Canadian Officials in Relation to Maher Arar*, 2007 F.C. 766 (Arar Commission) at paras. 37 *et seq.*

54 *CEA*, s. 38.13.

55 *CEA*, s. 38.131. The government urges that the Attorney General certificate process is necessary to bar release of information obtained in confidence under international intelligence-sharing arrangements (Government of Canada 2007, 16).

56 For an assessment of s. 38 of the *CEA*'s overall compliance with s. 7 of the Charter, see Grant (2003).

57 *CEA*, s. 38.14.

58 *Immigration and Refugee Protection Act* (*IRPA*), S.C. 2001, c. 27.

59 *IRPA*, ss. 76 *et seq.*

60 *IRPA*, s. 83(1)(e).

61 The men subject to security certificates at the time of this writing spent (and, in one case, continue to spend) lengthy periods incarcerated: by the beginning of 2007, the average period of detention for the men still imprisoned at that time was almost six years. This is a period of detention longer than the median sentence for *convicted attempted* murderers in Canada. In fact, it fell just short of the seven-year median sentence for convicted *murders* (see Statistics Canada, "Sentenced Cases and Outcomes in Adult Criminal Court, by Province and Yukon, 2003" (http://www40.statcan.ca/l01/cst01/legal21a.htm, accessed May 4, 2009). Almrei – the individual still in detention – has spent much of his period in jail in solitary confinement and, until relatively recently, in provincial detention facilities ill-equipped for long-term detentions. His period of detention is now longer than the median sentence in Canada for a convicted murderer.

62 *Charkaoui v. Canada*, 2007 S.C.C. 9.

63 Ibid. at para. 28.

64 Ibid. at para. 48.

65 Ibid. at para. 53.

66 R.S.C., 1985, c. O-5.

67 R.S.C., 1970, c. O-3. This Act, in turn, is an "adoption of the English statutes as enacted in Great Britain (1911 [U.K.] c. 28, and 1920 [U.K.], c. 75)." *R. v. Toronto Sun Publishing Limited*, (1979) 24 O.R. (2d) 621 at 623 (Ont. Prov. Ct.) [*Toronto Sun*].

68 *House of Commons Debates*, 096 (30 April 1998) at 1010 (Hon. Andy Scott).

69 *R v. Ratkai*, [1989] N.J. No. 334 (Nfld. S.C. [T.D.]) (Q.L.).

70 *Toronto Sun*, (1979) 24 O.R. (2d) 621 at 632. Notably, the question of ambiguity in the Act became the key point on which the Juliet O'Neill matter, described below, turned. By the time of the latter case, however, excessive ambiguity was unconstitutional, given the way in which section 7 of the Charter of Rights and Freedoms had been interpreted.

71 *SOIA*, s. 8 and accompanying schedule. Further, under section 10, other persons may be designated "a person permanently bound to secrecy" if certain senior government officials believe that "by reason of the person's office, position, duties, contract or arrangement...the person had, has or will have authorized access to special operational information; and...it is in the interest of national security to designate the person."

72 *SOIA*, s. 8.

73 *CSIS Act*, s. 18.

74 [1979] 1 S.C.R. 218 at 250–51.

75 *O'Neill v. Canada* (2006), 82 O.R. (3d) 241 (On. Sup. Ct of Jus.) at para. 62 and 71 (holding, *inter alia*, that section 4 failed "to define in any way the scope of what it protects and then, using the most extreme form of government control, criminalizes the conduct of those who communicate and receive government information that falls within its unlimited scope including the conduct of government officials and members of the public and of the press" and that "the lack of delineation of a zone of risk by these sections gives no guidance to law enforcement officials to be able to determine whether a crime has been committed under them, with the result that there are no controls on the exercise of their discretion and there is the danger of arbitrary and ad hoc law enforcement").

76 Information Commissioner of Canada (2002, 20). For an academic critique of the amendments, see McMahon (2002).

77 The same report acknowledges that the information in question was not "special operational information as defined by the *Security of Information Act*." In these circumstances, the only provisions of *SOIA* that could apply are sections 4 and 16. However, section 16 – which relates to information the government is "safeguarding" – is only triggered if the person communicates the information to a foreign entity or to a terrorist group in either an effort to harm Canadian interests (a defined concept that involves real risks) or if such harm actually occurs. There is absolutely no basis to conclude – and nothing in the DFAIT report to suggest – that Couillard was communicating the Bernier documents to a foreign entity or terrorist group. Even if she had, the DFAIT report asserts that "Our review of the documents in question concluded that their disclosure would not have caused significant injury to the national interest." Neither of the requirements for section 16 were, in other words, in play in the Bernier-Couillard matter. By default, the only provision of *SOIA* that could apply to Couillard's case would be the (unconstitutional) section 4.

78 1989 c. 6 [UK *Official Secrets Act*]. For a full discussion of the UK Act, see Wadham and Modi (2003).

79 UK *Official Secrets Act*, s. 1(1).

80 Ibid., s. 1(5).

81 Ibid., s. 1(4).

82 [2007] U.K.H.L 46.

83 For a summary of the effect of *MB*, see Carlile (2008).

84 See, for example, Toughill (2008); Pugliese (2008a, b, c); Naumetz (2008); Woods (2008); "Harper's Secrecy" (2008); "Too Much Secrecy" (2008); "Afghanistan: Selling the Mission's Merits" (2008); "Harper's Unwise Afghan Blackout" (2008); Mayeda (2007); "Secret Documents, Secret Challenges" (2007); "A Few More Bricks" (2007). In his 2007-08 report, the information commissioner reported receiving "more than 100 complaints in 2007-2008 from the media, members of Parliament, academics and the public related to access requests for information about various aspects of the Afghanistan mission, such as operations, related events and activities, treatment of detainees, and policies" (Information Commissioner of Canada 2008). The information commissioner expressed at least partial satisfaction with the government's performance on the Afghan file. For its part, the House of Commons Standing Committee on Access to Information, Privacy and Ethics flagged a number of concerns in the handling of at least one Afghan-related information request. See House of Commons Standing Committee on Access to Information, Privacy and Ethics (2008).

85 Order-in-Council, P.C. 2006-0293 (2006-05-01).

86 Order-in-Council, P.C. 2006-1526 (2006-12-11).

87 *Canada (Attorney General) v. Commission of Inquiry into the Action of Canadian Officials in Relation to Maher Arar*, 2007 F.C. 766 (F.C.) (Arar Commission) at para. 58.

88 *R. v. Khawaja*, 2007 F.C. 463 at para. 150 *varied* 2007 F.C.A. 388.

89 See, for example, ibid.; *Canada v. Kempo*, 2004 F.C. 1678 (F.C.); *Re Zundel*, 2005 F.C. 295 (F.C.); *Cemerlic v. Canada (Solicitor General)*, 2003 FCT 133 (F.C.); *Canada (Minister of Citizenship and Immigration) v. Singh*, [1998] F.C.J. No. 978 (F.C.T.D.); *Ternette v. Canada*, [1992] 2 F.C. 75 (F.C.T.D.); *Henrie v. Canada (Security Intelligence Review Committee)*, [1989] 2 F.C. 229, *aff'd* [1992] F.C.J. No. 100 (F.C.A.); *Re Jaballah*, [2003] 4 F.C. 345 (F.C.); *Ruby v. Canada (Solicitor General)*, [1998] 2 F.C. 351.

90 Reproduced in *Kempo*, 2004 F.C. 1678 at para. 62.

91 *Henrie*, [1989] 2 F.C. 229 at para. 29.

92 In this last regard, see Pozen (2005) for a sustained critique of how the mosaic effect has been employed in the United States.

93 *O'Neill*, [2004] O.J. No. 4649 at para. 69.

94 *Khadr v. Canada*, 2008 F.C. 549 at para. 77.

95 *Khawaja*, 2007 F.C. 463 at para. 136.

96 *Khadr*, 2008 F.C. 549 at para. 98.

97 See *Cemerlic*, 2003 F.C.T. 133 at paras. 18 *et seq.* (discussing s. 19 of the *Privacy Act*).

98 *Khawaja*, 2007 F.C. 463 at para. 146 ("it is not open to the Attorney General to merely claim that information cannot be disclosed pursuant to the third party rule, if a request for disclosure in some form has not in fact been made to the original foreign source").

99 Ibid. at para. 152.

100 Ibid. at para. 147; *Ottawa Citizen Group Inc. v. Canada (Attorney General)*, 2006 F.C. 1552 (F.C.) at para. 66.

101 *Khawaja*, 2007 F.C. 463 at para. 148.

102 *Charkaoui*, 2007 S.C.C. 9 at para. 87.

103 R.S.C., 1985, c. O-5.

104 Affidavit of Gordon Cameron, in *Almrei*, Court File DES-3-08, dated July 20, 2008 at para. 22.

105 Ibid. at para. 36.

106 *Charkaoui*, 2007 S.C.C. 9 at para. 83.

107 At the Commons committee hearing on Bill C-3, the government asserted a preference for the UK model because "the Supreme Court mandate was to make sure

that the special advocate represents the interests of the individual. The only living example of this was the UK special advocate system, so that was essentially how we got to the UK model as the starting point" (Daniel Therrien [acting Assistant Deputy Attorney General, Citizenship, Immigration and Public Safety Portfolio, Department of Justice], *Evidence*, 39th Parl., 2nd Sess., Tuesday, November 27, 2007). On a technical level, it is true that in the SIRC process, SIRC counsel represents the interests of SIRC, and those interests tend also then to dovetail with the complaint to the extent that both have an interest in the truth. The government's explanation for its reliance on the UK model does not, however, answer the question of why they did not graft onto that model the more rights-protecting aspects of the SIRC approach, not least in terms of continued access to the named person and robust full-disclosure powers.

108 Hon. Pierre Claude Nolin, *Debates of the Senate (Hansard)*, 39th Parl., 2nd Sess., volume 144, issue 32, Tuesday, February 12, 2008. In direct response to the scant time available to it when Bill C-3 was promulgated, the Special Senate Committee on *Anti-terrorism* is now engaged in an extensive, supplemental study of the security certificate process.

109 To be fair, the Special Senate Committee on the *Anti-terrorism Act* did discuss both the *SOIA* and the *CEA* in some detail in its 2007 report. Nothing, however, has happened since.

110 UK *Official Secrets Act*, s. 3(5).

References

"A Few More Bricks in Wall of Secrecy." 2007. *Toronto Star*, May 1, A14.

"Afghanistan: Selling the Mission's Merits." 2008. *Windsor Star*, January 25, A8.

Banisar, David. 2006. *Freedom of Information around the World 2006*. London: Privacy International. Accessed April 30, 2008. http://www.freedominfo.org/documents/global_survey2006.pdf

Brandeis, Louis D. 1914. *Other People's Money and How the Bankers Use It*. New York: Frederick A. Stokes Company.

Canadian Security Intelligence Service (CSIS). 2004. *Backgrounder 12 – Security of Information Act*. Accessed May 1, 2009. http://www.csis.gc.ca/nwsrm/bckgrndrs/bckgrndr12-eng.asp

———. 2005. *Backgrounder 1 – CSIS Mandate*. Accessed June 1, 2009. http://www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr01-eng.asp.

Carlile, Alex (Lord Carlile of Berriew). 2008. *Third Report of the Independent Reviewer Pursuant to Section 14(3) of the Prevention of Terrorism Act 2005*. Accessed April 31, 2009. http://security.homeoffice.gov.uk/news-publications/publication-search/general/report-control-orders-2008?view=Binary

Chevigny, Paul H. 1991. "Information, the Executive and the Politics of Information." In *Speech and National Security*, edited by Shimon Shetreet. Boston: Martinus Nijhoff Publishers.

Coliver, Sandra. 1999. "Commentary on the Johannesburg Principles on National Security, Freedom of Expression and Access to Information." In *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information*, edited by Sandra Coliver, Paul Hoffman, Joan Fitzpatrick, and Stephen Brown. The Hague: Martinus Nijhoff Publishers.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Commission). 2006. *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Ottawa: Public Works and Government Services Canada.

Forcese, Craig. 2008. "Fixing the Deficiencies of Parliament Review of Anti-terrorism Law: Lessons from the United Kingdom and Australia." *IRPP Choices* 14 (4). Accessed May 1, 2009. http://www.irpp.org/fasttrak/index.htm

Forcese, Craig, and Lorne Waldman. 2007. "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings." Study commissioned by the Canadian Centre for Intelligence and Security Studies. Accessed May 1, 2009. http://aix1.uottawa.ca/~cforcese/other/sastudy.pdf

Foreign Affairs and International Trade Canada. 2008. "Final Report on the Administrative Review into the Security Incident Reported by Maxime Bernier – Classified Documents Left at a Private Residence." Accessed May 1, 2009. http://www.international.gc.ca/about-a_propos/report-rapport.aspx

Government of Canada. 2007. "Government Response to the Seventh Report of the Standing Committee on Public Safety and National Security." 39th Parl., 1st Sess. Accessed May 1, 2009. http://www2.parl.gc.ca/ committeebusiness/ReportsResponses.aspx?Cmte=SECU&Language=E&Mode=1&Parl=39&Ses=1

Grant, Kathy. 2003. "The Unjust Impact of Canada's *Anti-terrorism Act* on an Accused's Right to Full Answer and Defence." *Windsor Review of Legal and Social Issues* 16: 137-68. Accessed May 1, 2009. http://faculty.law.ubc.ca/Pue/pdf/Kathy%20Grant%20anti%20terror%20evidence%20act.pdf

Hamilton, Lee. 1997. "Secrecy." *Congressional Record*, March 19, E514.

"Harper's Secrecy on Detainees." 2008. *Times Colonist*, January 26, A14.

"Harper's Unwise Afghan Blackout." 2008. *Toronto Star*, January 25, AA4.

House of Commons Standing Committee on Access to Information, Privacy and Ethics (Paul Szabo, Chair). 2008. "Access to Information Request for the Department of Foreign Affairs and International Trade Internal Report Entitled 'Afghanistan 2006: Good Governance, Democratic Development and Human Rights.'" 39th Parl., 2nd Sess., report 4. Accessed May 1, 2009. http://www2.parl.gc.ca/committeebusiness/ReportsResponses.aspx?Cmte=ETHI&Language=E&Mode=1&Parl=39&Ses=2

House of Commons Standing Committee on Justice and Solicitor General on the Review of the *Access to*

Information Act and the *Privacy Act*. 1987. *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. Ottawa: Queen's Printer.

House of Commons Standing Committee on Public Safety and National Security, Subcommittee on the Review of the *Anti-terrorism Act*. 2007. "Rights, Limits, Security: A Comprehensive Review of the *Anti-terrorism Act* and Related Issues," 39th Parl.,1st Sess., report 7. Accessed May 1, 2009. http://www2.parl.gc.ca/committeebusiness/ReportsResponses.aspx?Cmte=SECU&Language=E&Mode=1&Parl=39&Ses=1

Information Commissioner of Canada. 1998. *Annual Report 1997-1998*. Ottawa: Minister of Public Works and Government Services. Accessed May 1, 2009. http://www.infocom.gc.ca/reports/default-e.asp

———. 2000. *Annual Report 1999-2000*. Ottawa: Minister of Public Works and Government Services. Accessed May 1, 2009. http://www.infocom.gc.ca/reports/default-e.asp

———. 2001. *Annual Report 2000-2001*. Ottawa: Minister of Public Works and Government Services. Accessed May 1, 2009. http://www.infocom.gc.ca/reports/default-e.asp

———. 2002. *Annual Report 2001-2002*. Ottawa: Minister of Public Works and Government Services. Accessed May 1, 2009. http://www.infocom.gc.ca/reports/default-e.asp

———. 2008. *Annual Report 2007-2008*. Ottawa: Minister of Public Works and Government Services. Accessed May 1, 2009. http://www.infocom.gc.ca/reports/default-e.asp

Judd, Jim. 2007. "How Should a Democracy Respond to Domestic Terrorist Threats." Talking points for 2007 Raoul Wallenberg International Human Rights Symposium, January 19. Canadian Security Intelligence Service. Accessed May 1, 2009. http://www.csis.gc.ca/nwsrm/spchs/spch19012007-eng.asp

———. 2008. "Remarks at the Global Futures Forum Conference in Vancouver, May 15," Canadian Security Intelligence Service. Accessed May 1, 2009. http://www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp

Law Reform Commission of Canada. 1986. *Crimes against the State*. Ottawa: Law Reform Commission of Canada.

Lynch, Andrew. 2006. "Legislating with Urgency." *Melbourne University Law Review* 30 (3): 747. Accessed May 22, 2009. http://search.austlii.edu.au/au/journals/MULR/2006/24.html

Mackmurdo, Christopher. 2007. "Intelligence and International Security after 9/11." In *Understanding Global Terror*, edited by Christopher Ankersen and Michael O'Leary. Oxford, UK: Blackwell Publishing.

MacLeod, Ian. 2006. "Ruling Threatens Law That Lets CSIS Probe Terrorism." *Ottawa Citizen*, November 27.

Macnamara, W.D., and Ann Fitz-Gerald. 2002. "A National Security Framework for Canada." *IRPP Policy Matters* 3 (10).

Mayeda, Andrew. 2007. "MPs Push for Contract Details; Harper Government under Fire for Secrecy Surrounding Hired Contractors in Afghanistan." *Vancouver Sun*, November 26, A6.

McMahon, Patricia. 2002. "Amending the *Access to Information Act*: Does National Security Require the Proposed Amendments of Bill C-36?" *University of Toronto Faculty of Law Review* 60 (1): 89-101.

Naumetz, Tim. 2008. "Ombudsman Admits Aiding DND Secrecy; Afghan Detainees." *National Post*, May 28, A9.

Padover, S., ed. 1953. *The Complete Madison: His Basic Writings*. New York: Harper, cited in T. Murray Rankin,1979. *Freedom of Information in Canada: Will the Doors Stay Shut?* Ottawa: Canadian Bar Association.

Pozen, David E. 2005. "The Mosaic Theory, National Security, and the Freedom of Information Act." *Yale Law Journal* 115 (3): 628-79.

Presidential Documents. 2009. "Transparency and Open Government." *Federal Register* 74 (15): 4685-6. Accessed April 26, 2009. http://frwebgate4.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=857024457699+ 13+2+0&WAISaction=retrieve

Privy Council Office. 2004. *Securing an Open Society: Canada's National Security Policy*. Accessed May 1, 2009. http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf

Pugliese, David. 2006. "Ottawa Declares Publicly Available Data a State Secret." *Edmonton Journal*, October 4, A5.

_____. 2008a. "Once Public, Now Secret." *Ottawa Citizen*, June 16, A1.

_____. 2008b. "DND Releases Secret Files on Afghan Mission Ammo; Military Careful about Sharing Info Because Taliban Read Citizen, Top General Says." *Ottawa Citizen*, February 7, A1.

_____. 2008c. "Reasons for Secrecy Are Secret, Military Says; Canadian Forces Refuses to Give Details on Ammo Used in Afghanistan – or Say Why." *Ottawa Citizen*, February 5, A4.

Rankin, T. Murray 1979. *Freedom of Information in Canada: Will the Doors Stay Shut?* Ottawa: Canadian Bar Association.

Richelieu, Duc De. 1641. "Maxims." *Testament Politique*, cited in *The Columbia World of Quotations*, New York: Columbia University Press: 1996. Accessed May 1, 2009. http://www.bartleby.com/66/34/46534.html

Richelson, Jeffrey. 1999. *The U.S. Intelligence Community*. 4th ed. Boulder, CO: Westview Press.

Roach, Kent. 2008. "The Role and Capacities of Courts and Legislatures in Reviewing Canada's Anti-terrorism Law." *Windsor Review of Legal and Social Issues* 24:5-56.

———. Forthcoming. "Charkaoui and Bill C-3: Some Implications for Anti-terrorism Policy and Dialogue between Courts and Legislatures." *Supreme Court Law Review*.

Roberts, Alasdair. 2004. "National Security and Open Government." *Georgetown Public Policy Review* 9 (2): 69-85.

Rosenthal, Peter. 2003. "Disclosure to the Defence after September 11: Sections 37 and 38 of the *Canada Evidence Act*." *Criminal Law Quarterly* 48 (2): 186-204.

Royal Commission on Security. 1969. *Report of the Royal Commission on Security*. Ottawa: Queen's Printer.

"Secret Documents, Secret Challenges." 2007. *Globe and Mail*, August 8, A16.

Security Intelligence Review Committee. 1989. *Annual Report 1988-89*. Accessed May 1, 2009. http://www.sirc-csars.gc.ca/anrran/index-eng.html

Special Senate Committee on the *Anti-terrorism Act*. 2007. *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the* Anti-Terrorism Act. Accessed May 1, 2009. http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/anti-e/rep-e/rep02feb07-e.htm

Standing Senate Committee on National Security and Defence. 2003. *The Myth of Security at Canada's Airports*. Accessed May 4, 2009. http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.htm

"Statement by the President upon Signing Bill Revising Public Information Provisions of the Administrative Procedure Act." 1966. *Weekly Compilation of Presidential Documents* 895 (July 4). Accessed May 4, 2009. http://www.gpoaccess.gov/wcomp/index.html

Stewart, Hamish. 2003. "Public Interest Immunity after Bill C-36." *Criminal Law Quarterly* 47 (3): 249.

"Too Much Secrecy." 2008. *Winnipeg Free Press*, January 26, A18.

Toughill, Kelly. 2008. "Tentacles of Secrecy Grip Tightly." *Toronto Star*, August 9, AA6.

Treasury Board of Canada Secretariat. 2008. "Access to Information Requests – April 1, 2006 to March 31, 2007." InfoSource Bulletin no. 30. Accessed May 4, 2009. http://www.infosource.gc.ca/bulletin/2008/bulletin03-eng.asp

United States. Commission on Protecting and Reducing Government Secrecy.1997. *Report of the Commission on Protecting and Reducing Government Secrecy*. Senate Document 105-2. Washington, DC: Government Printing Office.

Wadham, John, and Kavita Modi. 2003. "National Security and Open Government in the United Kingdom." *National Security and Open Government: Striking the Right Balance*. Syracuse, NY: Campbell Public Affairs Institute. Accessed May 4, 2009. http://www.maxwell.syr.edu/campbell/events/pastevents.htm

Walsh, James Igoe. 2007. "Defection and Hierarchy in International Intelligence Sharing." *Journal of Public Policy* 27 (2): 151-81.

Wark, Wesley. 2001. "The *Access to Information Act* and the Security and Intelligence Community in Canada." Access to Information Review Task Force Report 20. Accessed May 4, 2009. http://www.atirtf-geai.gc.ca/paper-intelligence1-e.html

———. 2007. "It's Official: The Government Abused Its Secrecy Authority." *Globe and Mail*, August 10, A17.

Wichmann, Charles J., III. 1998. "Ridding *FOIA* of Those 'Unanticipated Consequences': Repaving a Necessary Road to Freedom." *Duke Law Journal* 47:1213-56.

Woods, Allan. 2008. "Watchdog Calls Detainee Inquiry; Says Tories Stalling Attempts to View Documents on Transfer of Afghan Prisoners." *Toronto Star*, March 13, A3.

Résumé

En matière d'information, le principal dilemme que rencontrent les gouvernements consiste à concilier l'intérêt public pour la divulgation de l'information et la légitime confidentialité de certains renseignements.

Dans cette étude, Craig Forcese évalue les efforts du Canada en vue de trouver un juste équilibre entre transparence et secret dans le domaine de la sécurité nationale. Il décrit d'abord les principes sur lesquels reposent les notions de « gouvernement transparent » et d'« audiences publiques », puis les principes de confidentialité en matière de sécurité nationale, c'est-à-dire les motifs qui sont invoqués pour justifier la nécessité de préserver le secret. L'auteur examine ensuite comment les lois en matière d'information au Canada protègent la confidentialité des questions de sécurité nationale et dans quelle mesure celles-ci réussissent à concilier les exigences de transparence et de sécurité nationale, en signalant certains problèmes pratiques et structurels qui compromettent cette conciliation. Ces problèmes font dire à l'auteur que les lois en matière d'information et leur mise en pratique laissent grandement à désirer au Canada.

Certaines observations des milieux mêmes du renseignement et de la sécurité amènent à penser que l'étendue de la confidentialité prévue dans les lois dépasse les besoins de protection légitime. L'incohérence de ces lois – de même que l'incertitude et les réclamations excessives qu'elles entraînent – crée des conditions susceptibles de freiner les échanges d'information utiles et de miner par conséquent la crédibilité des services de sécurité.

L'auteur note que les limites imposées par les lois encadrant l'accès à l'information – et les pénalités draconiennes prévues dans certains cas – sont nettement incompatibles avec la démocratie qu'elles sont censées protéger. Leur ambiguïté est telle qu'elles pourraient être utilisées par le gouvernement pour éviter les situations embarrassantes et masquer les cas d'incompétence, au nom de la sécurité nationale. Si cela se produisait, ces lois amoindriraient la confiance de la population, ce qui risquerait d'entraîner des correctifs qui rendraient plus difficile la protection de secrets légitimes. L'auteur formule en terminant une série de recommandations visant à concilier plus efficacement les exigences de secret et de transparence dans la pratique et le droit canadiens.

Summary

The dilemma of any government information regime lies in balancing the strong public interest in disclosure in all areas, including national security, against legitimate secrecy. In this study, Craig Forcese assesses Canada's efforts to balance transparency with secrecy in the national security area. He first highlights the principles of transparency that animate the Canadian concepts of open government and open courts. He then posits several principles of national security confidentiality – that is, justifications for secrecy predicated on national security preoccupations. He also describes how Canadian information laws seek to guard national security confidentiality. In the final section of the study, he assesses how well Canadian information law reconciles national security with transparency, identifying a number of structural and practical problems that plague this reconciliation.

Forcese concludes that Canada's information laws and practices leave much to be desired. Past commentary from the security and intelligence community suggests that secrecy laws are broader than is necessary to protect legitimate national security secrets. At the same time, the incoherence of these laws, the uncertainty this incoherence produces and the overclaiming it allows, create conditions that are likely to curb benign information exchanges. This would be at great expense to the credibility of the security services.

In addition, he says, the limits these laws impose on information access, and the draconian penalties they level in some instances, are deeply inconsistent with the very democracy they are supposed to protect. They are sufficiently ambiguous to let government sidestep embarrassment and mask incompetence, all in the name of national security. If they were used to this end, they would jeopardize confidence in government and potentially stimulate changes that make protecting legitimate secrets more difficult. The study concludes with a number of recommendations as to how secrecy and transparency might be reconciled better in Canadian law and practice.

Among other things, he urges Parliament to formally repeal section 4 of the *Security of Information Act* and replace it with a much more measured provision. He also calls on government to standardize its definition of "national security" across the statute book, to avoid the confusing array of terms that currently exist. Forcese also expresses support for a standing reviewer of national security law and policy, and a separate committee of parliamentarians with legislated powers and access to secret information.